

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-213104

(43) 公開日 平成11年(1999) 8月6日

(51) Int.Cl.⁶

識別記号

F I

G 0 6 K 17/00

G 0 6 K 17/00

B

S

T

G 0 6 F 17/60

G 0 7 B 5/00

A

G 0 7 B 5/00

15/00

U

審査請求 未請求 請求項の数29 O L (全 36 頁) 最終頁に続く

(21) 出願番号

特願平10-10312

(22) 出願日

平成10年(1998) 1月22日

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72) 発明者 中垣 寿平

神奈川県足柄上郡中井町境430 グリーン

テクナカイ 富士ゼロックス株式会社内

(72) 発明者 木子 健一郎

神奈川県足柄上郡中井町境430 グリーン

テクナカイ 富士ゼロックス株式会社内

(72) 発明者 京嶋 仁樹

神奈川県足柄上郡中井町境430 グリーン

テクナカイ 富士ゼロックス株式会社内

(74) 代理人 弁理士 澤田 俊夫

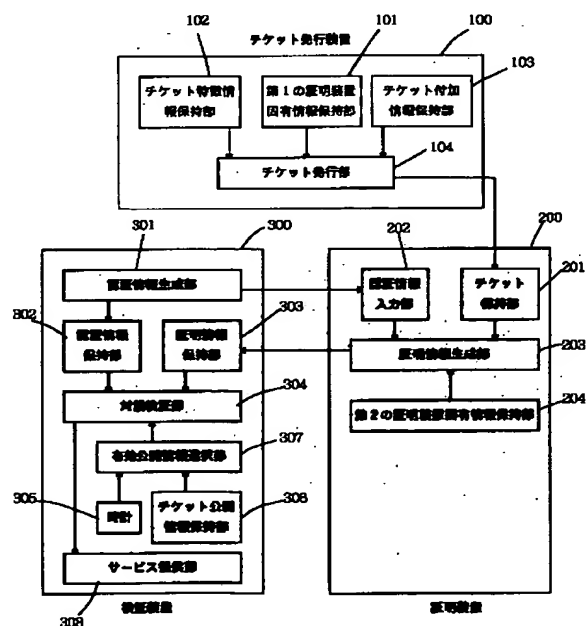
最終頁に続く

(54) 【発明の名称】 電子チケットシステム

(57) 【要約】

【課題】 証明装置および検証装置の間でチケット秘密情報に基づく対話証明を行なう際に、チケット秘密情報に有効期間を設け、チケット秘密情報が露呈した場合でも、被害を少なく押さえる。

【解決手段】 チケット発行装置100のチケット発行部104は、利用者の証明装置固有情報と、チケットの有効期間に応じて選択されたチケット秘密情報と、チケット付加情報とからチケットを生成する。証明装置200の証明情報生成部203は、検証装置300からの認証情報を元にして、対応するチケット、証明装置固有情報とを用いて証明情報を生成し、検証装置300へ送る。検証装置300の有効公開情報選択部307は、現時点で有効なチケット公開情報を選択し、対話検証部304は、証明情報保持部303に保持している証明情報が、認証情報に基づいて正当なチケットによって作成されていることを検証する。



第1の実施例における電子チケットシステムの構成

1

【特許請求の範囲】

【請求項1】 チケット発行装置、検証装置および証明装置からなる電子チケットシステムであって、

上記チケット発行装置は、

発行するチケットの秘密の特徴情報であるチケット秘密情報と上記チケット秘密情報の有効期間を表すチケット特徴情報有効期間とを対応させて保持するチケット特徴情報保持手段と、

利用者が保持する証明装置の固有情報を保持する第1の証明装置固有情報保持手段と、

発行するチケットの有効日または有効期間と上記チケット特徴情報保持手段に保持されているチケット特徴情報有効期間とに基づいて上記チケット秘密情報を選択し、上記選択したチケット秘密情報と上記第1の証明装置固有情報保持手段に保持している上記証明装置固有情報とを用いてデジタル情報であるチケットを作成するチケット発行手段とを有し、

上記証明装置は、

上記証明装置の固有情報を保持する第2の証明装置固有情報保持手段と、

上記チケット発行装置によって発行されたチケットを保持するチケット保持手段と、

上記第2の証明装置固有情報保持手段に保持している上記証明装置固有情報と、上記チケット保持手段に保持している上記チケットと、上記検証装置が生成した認証情報とを用いて証明情報を生成する証明情報生成手段とを有し、

上記検証装置は、

対話証明で用いられる値である認証情報を生成する認証情報生成手段と、

上記証明装置が生成した上記証明情報がチケット秘密情報に基づいて生成されていることを検証する対話検証手段とを有することを特徴とする電子チケットシステム。

【請求項2】 請求項1に記載の電子チケットシステムであって、

上記チケット発行手段は、

上記チケット特徴情報保持手段に保持されている上記チケット特徴情報有効期間のうち、発行するチケットの有効日または有効期間を含むものがある場合には、対応するチケット秘密情報と上記証明装置固有情報とを用いて

チケットを作成し、
含むものがない場合には、上記発行するチケットの有効期間をすべて含むように上記チケット特徴情報有効期間を組み合わせ、上記チケット特徴情報有効期間の組み合わせに対応するチケット秘密情報と上記証明装置固有情報とを用いて、複数のチケットを作成することを特徴とする電子チケットシステム。

【請求項3】 請求項1または2に記載の電子チケットシステムであって、上記チケット特徴情報有効期間は、他のチケット特徴情報有効期間と一部が重複するように

2

構成することを特徴とする電子チケットシステム。

【請求項4】 請求項1～3のいずれかに記載の電子チケットシステムであって、上記チケット特徴情報保持手段は、さらにチケットの公開の特徴情報であるチケット公開情報を対応させて保持し、上記チケット発行手段は、チケットを作成する際に、上記チケット秘密情報と上記証明装置固有情報と、さらに、対応するチケット公開情報とを用いてチケットを作成することを特徴とする電子チケットシステム。

10 【請求項5】 請求項4に記載の電子チケットシステムであって、上記チケット発行手段は、作成したチケットに上記チケット公開情報の一部を付加することを特徴とする電子チケットシステム。

【請求項6】 請求項1～3のいずれかに記載の電子チケットシステムであって、上記チケット特徴情報保持手段は、さらにチケットの公開の特徴情報であるチケット公開情報を対応させて保持し、上記チケット発行手段は、作成したチケットに上記チケット公開情報の一部を付加することを特徴とする電子チケットシステム。

20 【請求項7】 請求項1～6のいずれかに記載の電子チケットシステムであって、上記チケット公開情報には、上記チケット秘密情報を区別することができるチケット特徴情報識別子を含むことを特徴とする電子チケットシステム。

【請求項8】 請求項1～7のいずれかに記載の電子チケットシステムであって、

上記検証装置は、さらに上記チケット特徴情報有効期間とチケットの公開の特徴情報であるチケット公開情報との組からなる有効期限付きチケット公開情報を保持する

30 チケット公開情報保持手段と、
現在の日時を示す時計と、

上記チケット公開情報保持手段に保持されている上記有効期限付きチケット公開情報に含まれる上記チケット特徴情報有効期間と上記時計が示す日時とを比較して、現在の日時が含まれているものを選択する有効公開情報選択手段とを有し、

上記対話検証手段は、上記有効公開情報選択手段で選択された有効期限付きチケット公開情報に含まれるチケット公開情報を用いて上記証明情報がチケット秘密情報に基づいて生成されていることを検証することを特徴とする電子チケットシステム。

【請求項9】 請求項5～7のいずれかに記載の電子チケットシステムであって、

上記検証装置は、さらに上記チケット特徴情報有効期間とチケットの公開の特徴情報であるチケット公開情報との組からなる有効期限付きチケット公開情報を保持する

チケット公開情報保持手段と、

現在の日時を示す時計と、

上記チケット公開情報保持手段に保持されている上記有効期限付きチケット公開情報に含まれる上記チケット特

3

徴情報有効期間と上記時計が示す日時とを比較して、現在の日時が含まれているものを選択する有効公開情報選択手段とを有し、

上記認証情報生成手段は、上記有効公開情報選択手段で選択された有効期限付きチケット公開情報に含まれるチケット公開情報を用いて認証情報を生成し、

上記証明情報生成手段は、上記認証情報に含まれるチケット公開情報に基づいて上記チケット保持手段から使用するチケットを選択し、上記選択されたチケットと上記第2の証明装置固有情報保持手段に保持している上記証明装置固有情報と、上記検証装置が生成した認証情報とを用いて証明情報を生成し、

上記対話検証手段は、上記有効公開情報選択手段で選択された有効期限付きチケット公開情報に含まれるチケット公開情報を用いて上記証明情報がチケット秘密情報に基づいて生成されていることを検証することを特徴とする電子チケットシステム。

【請求項10】 請求項5～7のいずれかに記載の電子チケットシステムであって、

上記検証装置は、さらに上記チケット特徴情報有効期間とチケットの公開の特徴情報であるチケット公開情報との組からなる有効期限付きチケット公開情報を保持するチケット公開情報保持手段と、

現在の日時を示す時計と、

上記チケット公開情報保持手段に保持されている上記有効期限付きチケット公開情報に含まれる上記チケット特徴情報有効期間と上記時計が示す日時とを比較して、現在の日時が含まれているものをすべて抽出する有効公開情報選択手段とを有し、

上記認証情報生成手段は、上記有効公開情報選択で選択された各有効期限付きチケット公開情報に含まれるチケット公開情報を用いて複数の認証情報を生成し、

上記証明情報生成手段は、各認証情報に含まれるチケット公開情報に基づいて上記チケット保持手段から使用するチケットを検索し、該当するチケットが見つかったときにのみ該チケットと上記第2の証明装置固有情報保持手段に保持している上記証明装置固有情報と、上記検証装置が生成した認証情報とを用いて正しい証明情報を生成し、

上記対話検証手段は、上記正しい証明情報がチケット秘密情報に基づいて生成されていることを検証することを特徴とする電子チケットシステム。

【請求項11】 請求項5～7のいずれかに記載の電子チケットシステムであって、

上記検証装置は、さらに上記チケット特徴情報有効期間とチケットの公開の特徴情報であるチケット公開情報との組からなる有効期限付きチケット公開情報を保持するチケット公開情報保持手段と、

現在の日時を示す時計と、

上記チケット公開情報保持手段に保持されている上記有

4

効期限付きチケット公開情報に含まれる上記チケット特徴情報有効期間と上記時計が示す日時とを比較して、現在の日時が含まれているものをすべて抽出する有効公開情報選択手段とを有し、

上記証明情報生成手段は、上記チケット保持手段に保持している上記チケットに含まれるチケット公開情報の一部を、上記生成した証明情報に付加し、

上記対話検証手段は、上記証明情報に付加されている上記チケット公開情報が、上記有効公開情報選択手段で選択された有効期限付きチケット公開情報に含まれるチケット公開情報と一致するものがあるかどうかを検査し、一致するものがあつた場合にのみ、該チケット公開情報を用いて上記証明情報がチケット秘密情報に基づいて生成されていることを検証することを特徴とする電子チケットシステム。

【請求項12】 請求項1～7のいずれかに記載の電子チケットシステムであって、

上記検証装置は、さらに上記チケット特徴情報有効期間とチケットの公開の特徴情報であるチケット公開情報との組からなる有効期限付きチケット公開情報を保持するチケット公開情報保持手段と、

現在の日時を示す時計と、

上記チケット公開情報保持手段に保持されている上記有効期限付きチケット公開情報に含まれる上記チケット特徴情報有効期間と上記時計が示す日時とを比較して、現在の日時が含まれているものをすべて抽出する有効公開情報選択手段とを有し、

上記対話検証手段は、上記有効公開情報選択手段で選択された各有効期限付きチケット公開情報に含まれるチケット公開情報の各々を用いて上記証明情報がチケット秘密情報に基づいて生成されていることを検証し、1回でも検証が成功すれば、検証が成功したと判断することを特徴とする電子チケットシステム。

【請求項13】 請求項1～12のいずれかに記載の電子チケットシステムであって、

上記チケット発行装置は、さらに、チケットの利用条件などの情報を記述したチケット付加情報を保持するチケット付加情報保持手段を有し、

上記チケット発行手段は、チケット作成の際に、さらに上記チケット付加情報保持手段に保持している上記チケット付加情報も用いてチケットを作成し、

上記証明情報生成手段は、さらに上記チケット付加情報も用いて証明情報を生成することを特徴とする電子チケットシステム。

【請求項14】 請求項1～3のいずれかに記載の電子チケットシステムであって、上記チケット秘密情報は、公開鍵暗号方式における秘密情報からなることを特徴とする電子チケットシステム。

【請求項15】 請求項4～13のいずれかに記載の電子チケットシステムであって、上記チケット秘密情報

は、公開鍵暗号方式における秘密情報であり、上記チケット公開情報は、上記公開鍵暗号方式における秘密情報に対応する公開情報であることを特徴とする電子チケットシステム。

【請求項 16】 請求項 1～15 のいずれかに記載の電子チケットシステムであって、上記証明装置は、可変な内部状態を保持する内部状態保持手段を備えたことを特徴とする電子チケットシステム。

【請求項 17】 請求項 16 に記載の電子チケットシステムであって、上記証明装置の上記内部状態保持手段が保持する内部状態は、チケットと関連付けて保持されることを特徴とする電子チケットシステム。

【請求項 18】 請求項 17 に記載の電子チケットシステムであって、上記証明装置の上記内部状態保持手段は、チケットの有効性を示す内部状態をチケットと関連付けて保持し、上記証明装置の上記証明情報生成手段は、上記チケットの有効性を示す内部状態が特定の値であるときには、対応するチケットが無効であることを示す証明情報を生成することを特徴とする電子チケットシステム。

【請求項 19】 請求項 17 に記載の電子チケットシステムであって、上記証明装置の上記内部状態保持手段は、チケットの使用回数を表す内部状態をチケットと関連付けて保持し、上記証明装置の上記証明情報生成手段は、上記チケットの使用回数を表す内部状態を用いて演算した結果が特定の値であるときには、対応するチケットが無効であることを示す証明情報を生成することを特徴とする電子チケットシステム。

【請求項 20】 請求項 16～19 のいずれかに記載の電子チケットシステムであって、上記証明装置の上記内部状態保持手段が保持する内部状態の一部は外部から書き換え不能であることを特徴とする電子チケットシステム。

【請求項 21】 請求項 1～20 のいずれかに記載の電子チケットシステムであって、
上記証明装置は、さらに第 2 の認証情報を生成する第 2 の認証情報生成手段を有し、
上記検証装置は、さらに上記第 2 の認証情報生成手段が生成した上記第 2 の認証情報に対して、第 2 の証明情報を生成する第 2 の証明情報生成手段を有し、
上記証明装置は、さらに上記第 2 の認証情報と上記第 2 の証明情報とから、上記認証装置の正当性を検証することを特徴とする電子チケットシステム。

【請求項 22】 請求項 1～20 のいずれかに記載の電子チケットシステムであって、
上記証明装置は、さらに第 2 の認証情報を生成する第 2 の認証情報生成手段を有し、
上記検証装置は、さらに上記第 2 の認証情報生成手段が生成した上記第 2 の認証情報に対して、第 2 の証明情報を生成する第 2 の証明情報生成手段を有し、

上記証明装置は、さらに上記第 2 の認証情報と上記第 2 の証明情報と上記チケット付加情報とから、上記第 2 の証明情報の正当性を検証することを特徴とする電子チケットシステム。

【請求項 23】 請求項 21 または 22 のいずれかに記載の電子チケットシステムであって、上記証明装置は、上記第 2 の証明情報の正当性の検証に成功した場合、上記証明装置の内部状態を更新することを特徴とする電子チケットシステム。

10 【請求項 24】 請求項 1～23 のいずれかに記載の電子チケットシステムであって、上記証明装置の上記第 2 の証明装置固有情報保持手段と上記証明情報生成手段とは、内部のデータおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保持されていることを特徴とする電子チケットシステム。

20 【請求項 25】 請求項 1～24 のいずれかに記載の電子チケットシステムであって、上記証明装置の上記第 2 の証明装置固有情報保持手段と上記証明情報生成手段とは、IC カードなどの携帯可能な小型演算装置として構成されていることを特徴とする電子チケットシステム。

【請求項 26】 請求項 1～24 のいずれかに記載の電子チケットシステムであって、上記証明装置は、IC カードなどの携帯可能な小型演算装置として構成されていることを特徴とする電子チケットシステム。

【請求項 27】 発行するチケットの秘密の特徴情報であるチケット秘密情報と上記チケット秘密情報の有効期間を表すチケット特徴情報有効期間とを対応させて保持するチケット特徴情報保持手段と、
利用者が保持する証明装置の固有情報を保持する証明装置固有情報保持手段と、

30 発行するチケットの有効日または有効期間と上記チケット特徴情報保持手段に保持されているチケット特徴情報有効期間とに基づいて上記チケット秘密情報を選択し、上記選択したチケット秘密情報と上記証明装置固有情報保持手段に保持している上記証明装置固有情報とを用いてデジタル情報である電子チケットを作成するチケット発行手段とを有することを特徴とする電子チケット発行装置。

40 【請求項 28】 証明装置本体の固有情報を保持する証明装置固有情報保持手段と、
チケットの有効期間に関連付けられたチケット秘密情報と、証明装置本体の固有情報とに基づいて発行されたチケットを保持するチケット保持手段と、

上記証明装置固有情報保持手段に保持している上記証明装置固有情報と、上記チケット保持手段に保持している上記チケットとから、上記チケット秘密情報無しには生成できない証明情報を生成する証明情報生成手段とを有することを特徴とする電子チケット証明装置。

50 【請求項 29】 電子チケット証明装置により生成された証明情報を検証する電子チケット検証装置において、

認証情報を生成する認証情報生成手段と、
上記認証情報に基づいて上記証明装置が生成した証明情
報がチケット秘密情報に基づいて生成されていることを
検証する対話検証手段と、
上記対話検証手段の検証を、期間の有効なチケット秘密
情報に関してのみ成功裏に行なう手段とを有することを
特徴とする電子チケット検証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、チケットやカード 10
の作成、発行および利用の技術に関する。

【0002】

【従来の技術】乗車券、通行券、入場券、指定券、予約
券、回数券、定期券、商品券、プリペイドカード、ポイ
ントカード、会員証、通行証、許可証などは、それを保
持する利用者が、それに応じた各々の権利を保持するこ
とを証明する。ここでは、これらをまとめてチケットと
呼ぶ。一般にチケットは、権利を与える者もしくはその
代理人（以下ではまとめて発行者と呼ぶ）が発行して、
利用者が保持管理する。従来、チケットは、紙やプラス 20
チックなどへ印刷やエンボス加工などの処理を施すこと
で実現されていた。

【0003】このようなチケットをここでは紙チケット
と呼ぶ。これに対して、近年では、発行者が利用者に与
えた権利を特定できて、正しいチケットであることを検
証できるという機能を持つ電子チケットを実現する試み
がなされている。電子情報は、作成が容易であり、通信
回線を通して送信できるという特徴を持つ。しかしなが
ら、完全なコピーを簡単に作れるので、電子チケットを
実現するには、偽造と複製による不正利用への対策が必要である。電子署名の技術を用いることにより偽造は防
止できるが、複製の防止は困難であり、複製による不正
利用を防止することが、電子チケットの実現にあたって
の最大の課題となっていた。

【0004】この問題に対する、解決策として、従来、
チケットの利用時に正当な利用者か確認する第1の従来
技術、発行者以外の者にチケットを複写する機会を与え
ない第2の従来技術、検証時の通信を公開できるように
第2の従来技術を修正した第3の従来技術の3つの方法
が提案されてきた。

【0005】第1の従来技術は、チケットの利用時に、
利用者が正当な利用者かどうかを確認する方法であり、
利用者は、チケットを利用する時に、チケットとともに
自分が利用者特定情報に適合する正当な利用者であるこ
とを示す。利用者特定情報に適合していれば、対応する
権利の行使が認められる。確認のために必要な情報（利
用者特定情報）と、与えた権利とを対応づける情報がチ
ケットとして発行され、利用者が記録管理する。発行者
以外の者が勝手にチケットを偽造できないようにするた
めには、発行者がチケットに電子署名を施す。電子署名 50

のないチケットは、偽造されたものと判断される。利用
者特定情報には、身元、顔写真などの身体的特徴、パス
ワードなどの知識の所有、などが利用できる。

【0006】しかしながらこの方法では、利用する利用
者特定情報に応じて、いくつかの問題点が生ずる。

【0007】例えば、利用者特定情報に利用者の身元を
利用する方法では、発行時と検証時に利用者の身元が明
らかになり、匿名性が失われてしまう。また、通信回線
を利用した遠隔的な環境で身分を安全に証明する方法は
実現されていないので、このような環境では正当な権利
を持たないものが、不当にチケットを利用することを防
止することができない。

【0008】利用者特定情報にパスワードを利用すれ
ば、匿名性の問題は軽減されるが、パスワードを記憶す
る負荷を利用者にあたえる。また、利用者が故意にパス
ワードを漏洩させることを防止できないので、不正利用
の危険が増してしまうという問題点もある。

【0009】第2の従来技術は、例えば特開平8-14
7500号公報に示されるようなものであり、発行者以
外の者にチケットを複写する機会を与えない方法であ
る。この方法では、利用者が保持管理しているチケット
を複写できないようにする機構と、発行時や検証時の通
信からチケットが漏洩しない機構の両方を必要とする。

【0010】しかしながら、この方法では、（1）発行
者以外の者はチケットを複写できないので、チケットの
正当性を第三者に証明することが困難になる、（2）チ
ケットの発行時と検証時の通信の内容も機密に行うの
で、チケットの発行時と検証時にプライバシーなどの利
用者の権利が侵害されていないことを証明できない、と
いった問題点が生ずる。

【0011】第3の従来技術は、例えば特公平6-52
518号公報に示されるようなものであり、検証時の通
信を公開できるように第2の従来技術を修正した方法で
ある。この方法では、第2の従来技術と同様に、チケッ
トを秘密情報として利用者の所持する装置（証明器）に
複写できないように記録するが、検証の方法が異なる。
まず、検証を行う検証器は、証明器に乱数などの繰り返
し利用されない値（チャレンジ）を送る。証明器は、チ
ケットである秘密情報を利用した演算をチャレンジに対
して施して、得られた値（レスポンス）を検証器に送り
返す。検証器は、秘密情報とチャレンジを利用してレス
ポンスが演算されたことを確認することで、利用者の正
当性を認証する。レスポンスから逆に秘密情報を求める
ことを計算量的に困難とすることで、チャレンジとレス
ポンスを秘密通信とする必要がなくなる。

【0012】この方法は、認証のために利用されるもの
であり、正当なチケットを保持しているか否か以外に情
報を伝達しない。このため、有効期限などを示すことが
できず、単純なチケットしか表現できない。また、チケ
ットを証明器に送信する方法が、第2の従来技術と同様

に機密通信で行う必要があり、不当に利用者の情報を開示して利用者の権利を侵害していないことを証明できないという問題があった。

【0013】このように、従来の技術はいずれも、チケットに必要な不正利用を防止する機能を実現するために、第三者に対するチケットの内容証明の機能や利用者の匿名性を犠牲にしている点に問題があった。

【0014】これらの問題を解決する関連技術として、特願平9-188064号（平成9年7月14日出願、未公開）に示す方法が提案されている。この方法では、各利用者に、固有情報を封入した証明装置を持たせ、チケットはその証明装置固有情報とチケットの秘密情報とから生成して発行する。検証時には、検証装置が乱数などを用いて発行した値（チャレンジ）に対して、証明装置がチケットを用いて値（レスポンス）を検証器に送り返すことによって、正当なチケットを保持しているかどうかの検証を行う。正当なチケットと正当な証明装置の組み合わせのみが、正当なレスポンスを計算することが可能になる。

【0015】この方法では、チケットは秘密情報が取り出せないように構成されており、また他の証明装置と組にして利用しようとしても、利用できないようになっている。また、証明装置が検証装置に送る値（レスポンス）には、利用者が持つ証明装置の証明装置固有情報や利用者自身の情報は含まれることがないように構成できるので、利用者の匿名性も保つことが可能である。さらに、検証は、公開情報のみを用いて行うことが可能なので、利用者自身や第三者がチケットの正当性を確認することが可能である。

【0016】このように、この関連技術の方法を使うと、電子チケットの基本的な機能をすべて満たした安全な電子チケットを実現することができ、上記の問題をすべて解決することが可能である。

【0017】

【関連技術の問題点】上述したように、先の関連技術の方法を使うと、電子チケットの基本的な機能をすべて満たした安全な電子チケットを実現することができる。

【0018】しかし、この関連技術の方法では、チケット生成の際に使うチケット秘密情報が、万一漏洩してしまうと、正しい証明装置を持たなくても証明情報を計算することが可能になり、証明装置の詐称、およびチケットの詐称が可能になる。

【0019】例えば、公開鍵暗号RSA（Rivest Shamir Adelman）をベースにしたものを例にとると、万一、チケット秘密情報Dが露呈すると正しい証明装置を持たなくても証明情報を計算することが可能になり、証明装置の詐称、およびチケットの詐称が可能になる。直接、チケット秘密情報Dが露呈しなくても、法数nの素因数p、qが計算できてしまうと、チケット公開情報Eからチケット秘密情報Dを計算するこ

とが可能になり、同様に、証明装置の詐称、およびチケットの詐称が可能になる。

【0020】

【発明が解決しようとする課題】そこで、万一、チケット秘密情報が露呈した場合でも、被害を少なく押さえるために、ある一定期間毎にチケット秘密情報を変更したり、チケットの種別毎にチケット秘密情報を変更したりする方法が考えられる。

【0021】しかし、チケット秘密情報を変えると、当然今まで発行したチケットも使えなくなるため、問題が生じる。また一定期間毎にチケット秘密情報を変更する場合などには、チケット秘密情報の変更のタイミングよりも長い有効期間を持つチケットを発行し、運用しようとする問題が生じる。例えば、1ヶ月毎にチケット秘密情報を変更する場合には、半年間有効な定期券や、1年間有効な回数券や、3年間有効な会員権や、半年先の指定券などを発行する際に問題が生じる。また、チケットの種別毎にチケット秘密情報を変える場合にも、同じ検証装置で複数の種類のチケットを検証しようとする

【0022】

【課題を解決するための手段】本発明に係わる電子チケットシステムは、チケット発行装置、検証装置、証明装置からなる。チケットを発行するチケット発行装置は、発行するチケットの秘密の特徴情報であるチケット秘密情報と上記チケット秘密情報の有効期間を表すチケット特徴情報有効期間とを対応させて保持するチケット特徴情報保持手段を有し、発行するチケットの有効期間に合わせたチケット特徴情報を用いてチケットを発行する。一方、検証装置は、同様に上記チケット特徴情報有効期間とチケットの公開の特徴情報であるチケット公開情報との組からなる有効期限付きチケット公開情報を保持するチケット公開情報保持手段を有し、検証を行う日時に合わせたチケット公開情報を用いて検証を行う。

【0023】また、チケットの有効期間がチケット特徴情報有効期間の変更のタイミングよりも長い場合には、複数枚のチケットに分割して発行し、検証時には適切なチケットを選択して検証を行う。

【0024】さらに、万一チケット秘密情報が露呈した場合に、即座に他のチケット秘密情報によるチケット発行に切り替えることができるように、上記チケット特徴情報有効期間を、一部期間が互いに重複するように構成する。このように構成すると、同時期に複数の有効なチケット特徴情報が存在することになるため、検証装置と証明装置の対話証明の際に、認証情報や証明情報に、チケット公開情報の一部やチケット特徴情報識別子などを含ませて、どのチケット特徴情報による検証を行うのかを特定できるように構成する。

【0025】

【発明の実施の態様】以下、本発明を詳細に説明する。
 【0026】【第1の実施例】以下、本発明の実施例について説明する。

【0027】図1は、本発明の第1の実施例の電子チケットシステムの構成図である。第1の実施例では、チケットを作成する際のチケット秘密鍵を一定期間毎に一斉に変更するようにしている。

【0028】図1において、電子チケットシステムは、チケット発行装置100、証明装置200、検証装置300を含んで構成されている。

【0029】この図において、チケット発行装置100は利用者からの要求に応じてチケットを作成発行するものである。

【0030】証明装置200は、利用者が保持するものであり、例えばICカードのように内部に計算機能を持った携帯型の装置である。ICカード以外にも、計算機能を持ったPCカードや、携帯型情報ツールや、サブノートパソコンなどでもよいし、あるいは計算機能を持った時計や指輪などのように利用者が常に身につけているものでもよい。証明装置200は、内部の情報が、外部から簡単に改竄されたりすることがないように防御されていることが望ましい。

【0031】検証装置300は、利用者が正当な証明装置と正当なチケットとを持っていることを対話により検証する装置であり、正当だと判断すれば利用者にサービスを提供する。例えば鉄道の改札機、映画館の入場ゲート、デパートの会員証検査機などである。

【0032】チケット発行装置100は、利用者からの要求に応じてチケットを作成発行するものであり、第1の証明装置固有情報保持部101と、チケット特徴情報保持部102と、チケット付加情報保持部103と、チケット発行部104とから構成される。

【0033】第1の証明装置固有情報保持部101は、利用者が保持する証明装置200に封入されている証明装置固有情報の複製を保持するもので、利用者識別番号と利用者の証明装置固有情報との組で保持している。

【0034】チケット特徴情報保持部102は、チケットを発行する際に用いるチケット秘密情報を保持するもので、発行するチケットの有効期間にあわせて選択できるように、チケット秘密情報の有効期間を表すチケット特徴情報有効期間とチケット秘密情報とを対応させて保持している。

【0035】チケット付加情報保持部103は、チケットの利用条件などの付加的情報を記述したチケット付加情報を保持している。チケット付加情報は、例えばチケットの種類、指定券の日時、指定席の番号、チケット発行場所、コンサートの名称などチケットに付随するさまざまな情報を保持することができる。

【0036】チケット発行部104は、利用者から要求されたチケットを生成する部分であり、発行を要求した

利用者の証明装置固有情報と、チケットの有効日または有効期間にあわせて選択されたチケット秘密情報と、チケット付加情報とからチケットを生成する。

【0037】証明装置200は、チケット保持部201と、認証情報入力部202と、証明情報生成部203と、第2の証明装置固有情報保持部204とから構成される。

【0038】チケット保持部201は、チケット発行装置100から発行された複数のチケットを保持する部分である。

【0039】認証情報入力部202は、検証装置300から送られてくる認証情報を入力し保持する部分である。

【0040】第2の証明装置固有情報保持部204は、利用者毎の秘密情報を保持する部分であり、利用者毎に異なる証明装置固有情報を保持する。証明装置固有情報は証明装置200が作成された時に封入され、利用者にも容易に読み書きできないように構成されていることが望ましい。

【0041】証明情報生成部203は、認証情報入力部202に入力された認証情報を元にして、対応するチケット、証明装置固有情報とを用いて証明情報を生成し、検証装置300へ送る。

【0042】検証装置300は、認証情報生成部301と、認証情報保持部302と、証明情報保持部303と、対話検証部304と、時計305と、チケット公開情報保持部306と、有効公開情報選択部307と、サービス提供部308とから構成される。

【0043】認証情報生成部301は、証明装置200との間で対話して正当なチケットを保持していることを検証するための認証情報を生成する部分であり、リプレイ攻撃を防ぐために乱数などを用いて生成することが望ましい。

【0044】認証情報保持部302は、後に対話検証部304で検証の際に用いるために、認証情報生成部301で生成した認証情報を保持する部分である。

【0045】証明情報保持部303は、証明装置200で生成した証明情報を入力して保持する部分である。

【0046】時計305は、現在の日時を示す部分である。

【0047】チケット公開情報保持部306は、チケット特徴情報有効期間とチケットの公開情報との組からなる有効期限付きチケット公開情報を保持する部分である。チケット特徴情報有効期間は、チケット発行装置100のチケット特徴情報保持部102が保持しているチケット特徴情報有効期間と同じ物で、同じチケット特徴情報有効期間に対応するチケット秘密情報とチケット公開情報とが対応している。

【0048】有効公開情報選択部307は、現時点で有効なチケット公開情報を1つだけ選択する部分であり、

チケット公開情報の選択には、利用時の日時と、チケット公開情報保持部306のチケット特徴情報有効期間とを対比させて、適切な情報を選択する。

【0049】対話検証部304は、証明情報保持部303に保持している証明情報が、認証情報に基づいて正当なチケットと正当な証明装置200とによって作成されていることを検証する部分である。正当な証明情報は、チケット秘密情報による処理がなされているはずなので、検証はチケット秘密情報に対応するチケット公開情報を用いて行う。このチケット公開情報は、有効公開情報選択部307により選択されたものを用いる。

【0050】サービス提供部308は、対話検証部304による検証が正しいと判定された時に、利用者に対してサービスを提供する部分である。

【0051】次に、具体例を挙げて詳細に説明する。この説明では、公開鍵暗号方式のRSA暗号をベースにした例において、法数 n および秘密鍵 D を1ヶ月毎に変更する例について説明する。

【0052】RSA暗号では、 p 、 q を大きな素数、 n を法数、 $\Phi(n)$ をオイラー数、 E を公開鍵、 D を秘密鍵とするとき、以下の関係が成り立つ。 p 、 q を大きな素数、 n を法数とするとき、

【0053】

【数1】 $n = pq$

$\Phi(n) = (p-1)(q-1)$

$ED \equiv 1 \pmod{\Phi(n)}$

本実施例では、法数 n および秘密鍵 D を1ヶ月毎に変更するために、チケット発行装置100は、数ヶ月先までの毎月の法数 n と秘密鍵 D のリストを有し、発行を要求された日時のチケットをそのリストを元に適切な法数 n と秘密鍵 D を用いて作成する。証明装置200は、使用する日に使用可能なチケットを選択し、そのチケットを用いて証明情報を作成する。チケットの選択は証明装置200の所有者が選択してもよいし、証明装置200内に時計を有し、その日時情報を元に選択しても構わない。検証装置300は、現在有効な法数 n と公開鍵 E を保持しており、その法数 n と公開鍵 E を用いて、証明装置200から送られてくる証明情報を検証し、検証が成功すればサービスを提供する。検証装置300が有効な法数 n と公開鍵 E を知る方法としては、検証装置300の管理者が毎月外部から入力更新してもよいし、検証装置300が数ヶ月先までの毎月の法数 n と公開鍵 E のリストを所持していてもよい。

【0054】図2は、図1の構成図に記号を付けたものである。記号は以下の説明と対応している。本説明では、あるコンサートのチケットを発行し、検証するチケットシステムについて説明する。

【0055】チケット発行装置100のチケット付加情報保持部103は、チケット付加情報 L を保持している。チケット付加情報 L には、コンサートの名称、開催

会場、日時、指定席の番号、チケットの発行場所などの情報が含まれている。

【0056】チケット特徴情報保持部102には、図3に示すようにチケット秘密情報の有効期間を表すチケット特徴情報有効期間とチケット秘密情報とを対応させて保持している。図3では、例えば1997. 7. 1~1997. 7. 31の期間に有効なチケットを発行する際には、 $D7$ というチケット秘密鍵と法数 $n7$ とを用いてチケットを作成するということを示している。

10 【0057】第1の証明装置固有情報保持部101は、利用者識別番号と利用者の証明装置固有情報との組を保持している。第1の証明装置固有情報保持部101の例を図4に示す。

【0058】利用者識別番号が003である利用者から、1997年10月10日のコンサートのチケットの発行要求があったときのチケットの発行手順を、図5のフローチャートに沿って説明する。

【0059】(ステップS11) チケット発行部100は、チケット発行要求元の利用者の利用者番号を元に、第1の証明装置固有情報保持部101を検索して利用者の証明装置固有情報を検索する。いま、第1の証明装置固有情報保持部101の内容が図4に示すものであるとすると、利用者識別番号が003であるので、証明装置固有情報 $d003$ を検索する。

【0060】(ステップS12) チケット発行部100は、チケット付加情報保持部103から発行するチケットに適した付加情報 L を得る。ここでは、チケット付加情報 $L301$ は以下のような情報であるとする。

【0061】

【表1】

コンサート名称:	ABCコンサート、
開催会場:	XYZホール、
日時:	1997年10月10日
指定席:	123番
発行場所:	横浜チケットセンター

【0062】(ステップS13) チケット発行部100は、チケット特徴情報保持部102からチケットの指定日時に相当するチケット秘密情報(D , n)を検索する。いま、チケット特徴情報保持部102の内容が図3に示すものであるとすると、チケットの指定日時は1997年10月10日であるので、チケット秘密情報 $D10$ と法数 $n10$ を検索する。

【0063】(ステップ4) チケット発行部100は、証明装置固有情報 du とチケット秘密情報(D , n)とチケット付加情報 L とからチケットを生成する。チケット発行は以下の式により行う。

【0064】

【数2】 $t = D - F(n, L, du)$

ここで、関数 $F()$ は一方方向性関数であり、一方方向性ハッシュ関数MD5、SHAや、共通鍵暗号DES(Da

ta Encryption Standard)などを用いることができる。ここではチケットが上記の情報を元にして以下の式で表現される。

【0065】

【数3】

$t301 = D10 - F(n10, L301, d003)$

【0066】(ステップS15) チケット発行装置100は、上記のようにして作成したチケットtを、法数nおよびチケット付加情報Lと組にして、(t, n, L)の形式で発行する。上記の例の場合には、(t301, n10, L301)をチケットとして発行する。

【0067】次に、証明装置200について説明する。ここでは発行されたチケットは既にチケット保持部201に保持されているということを前提にする。また、チケット保持部201に保持されている複数のチケットの中から、利用者が利用するチケットを予め選択しているとする。チケットを予め選択するのは、自宅のパソコンなどにICカードとして実現されている証明装置を挿入して、パソコンの画面上で選択しておいてもよいし、ICカードを装着できる携帯型の簡易ビューワを用いて選択しておいてもよい。携帯型の簡易ビューワでは、例えば、複数のチケットのチケット付加情報を表示させて、適切なチケットを選択できるように構成すればよい。また、ここでは説明しないが、証明装置200に時計を設け、チケットを利用する時の日時と、チケット付加情報に含まれている日時とを比較して、適切なチケットを選択するように構成してもよい。

【0068】証明装置200の処理の流れを、利用者識別番号が003である利用者が所有する証明装置200を例にとって、図6に基づいて説明する。

【0069】(ステップS21) 証明装置200は、検証装置300から認証情報Cを受け取る。

【0070】(ステップS22) 証明装置200の証明情報生成部203は、チケット保持部201から選択されたチケット(t, n, L)を得、第2の証明装置固有情報保持部204から証明装置固有情報duを得る。ここでは、チケットとして、(t301, n10, L301)が得られ、証明装置固有情報としてd003が得られる。

【0071】(ステップS23) 証明装置200の証明情報生成部203は、これらの情報に基づいて、証明情報Rを生成して、検証装置300に送る。証明情報Rの計算式は以下の通りである。

【0072】

【数4】 $R = C^t C^{F(n, L, du)} \text{ mod } n$

ここでは、

【0073】

【数5】

$R = C^{t301} C^{F(n10, L301, d003)} \text{ mod } n10$

として、認証情報が生成される。

【0074】次に、検証装置300について説明する。ここでは、検証装置300が、コンサート会場の入り口に設置されたゲートで、利用者が挿入口に証明装置200であるICカードを挿入すると、対話検証を行い、検証の結果、正しいと判断すると、ゲートを開いて、利用者が入場できるものとする。ここでは、このゲートの開閉をサービスと呼び、サービス提供部308によって提供されるものとする。なお、ここでは自動ゲートとして説明するが、検証装置300は必ずしもそのような形式のものではなくてよく、例えばICカード挿入口が付いたパソコンでも構わない。利用者がパソコンに証明装置200であるICカードを挿入すると、パソコンは対話検証を行い、検証の結果、正しいと判断すると、「OK」などのメッセージを表示し、それを係員が見て、利用者を入場させるなどの構成でも構わない。

【0075】検証装置の処理の流れを図7に基づいて説明する。

【0076】(ステップS31) 検証装置300に証明装置200が挿入されると、検証装置300は認証情報生成部301で認証情報Cを生成し、認証情報保持部302に保持するとともに、証明装置200に送る。認証情報は、不正な攻撃者によるリプレイ攻撃を防ぐために、毎回異なっていることが望ましく、乱数などを含んで生成されるのが望ましい。ここでは、乱数を生成し、その乱数を認証情報とする。

【0077】(ステップS32) 検証装置300の有効公開情報選択部307は、時計305から現在の日時を入手し、その日時を元に、チケット公開情報保持部306から、現在有効なチケット公開情報(E, n)を1つだけ選択する。

【0078】ここでは、1997年10月10日のコンサートのチケットを、会場の入り口で検証しようとしており、現在の日時は1997年10月10日であるとする。また、チケット公開情報保持部306は図8に示す情報を保持しているものとする。このとき、有効公開情報選択部は、チケット公開情報保持部のチケット特徴情報有効期間と、現在の日時1997年10月10日とを比較し、

【0079】

【数6】 $(E10, n10)$

を選択する。

【0080】(ステップS33) 対話検証部304は、証明装置200から送られてきた証明情報Rと、認証情報保持部302に保持している認証情報Cと、有効公開情報選択部307により選択されたチケット公開情報(E, n)とを用いて、検証を行う。検証の手順は、以下の式の右辺と左辺とが等しいかどうかにより行う。

【0081】

【数7】 $C \equiv ? R^E \text{ mod } n$

証明情報Rが正当な証明装置と正当なチケットとを用い

で、正しく計算されているときには、上記の式の両辺が等しくなる。

【0082】

【数8】

$$\begin{aligned} R^E &\equiv (C^t C^{F(n, L, du)})^E \\ &\equiv (C^{D-F(n, L, du)} C^{F(n, L, du)})^E \\ &\equiv (C^D)^E \\ &\equiv C^{DE} \\ &\equiv C \pmod{n} \end{aligned}$$

ここでは、

【0083】

【数9】

$$R = C^{t301} C^{F(n10, L301, d003)} \pmod{n10}$$

であり、チケット公開情報としては (E10, n10) が選択されているので、

【0084】

【数10】

$$R^{E10} \equiv C^{D10 E10}$$

$$\equiv C \pmod{n10}$$

が成り立ち、検証が成功する。

【0085】（ステップS34）サービス提供部308は、対話検証部304による検証が成功すれば、ステップS35に進んで利用者にサービスを提供し、失敗すればそのまま終了する。

【0086】（ステップS35）利用者にサービスを提供する。ここでは、コンサート会場の入場ゲートを開く。

【0087】以上、第1の実施例においては、法数nおよび秘密鍵Dを一定期間毎に変更する例について、コンサートチケットを例にして説明した。予約券、指定券などの有効期間が短い（1日から数日）チケットに適用する場合には、同様の方法でチケットを発行することが可能である。

【0088】〔第2の実施例〕第2の実施例においては、第1の実施例と同様に、法数nおよび秘密鍵Dを一定期間毎に一斉に変更する例について、定期券や回数券などのように、有効期間が長いチケットへの適用について説明する。

【0089】定期券や回数券などのように有効期間が長いチケットでは、第1の実施例と同じように法数nを1ヶ月毎に変更するとすると、6ヶ月間有効な定期券や回数券などを発行する際には、問題となる。このような場合には、1ヶ月毎の複数のチケットに分割してチケットを作成する。

【0090】以下では第1の実施例の図を用いながら、異なる部分に焦点をあてて説明する。異なる部分は、チケット発行装置100であり、その他の部分や全体の構成は第1の実施例と同じである。

【0091】第2の実施例におけるチケット発行手順を、図9のフローチャートに示す。

【0092】（ステップS41）チケット発行部104は、チケット発行要求元の利用者の利用者番号を元に、第1の証明装置固有情報保持部101を検索して利用者の証明装置固有情報を検索する。

【0093】（ステップS42）チケット発行部104は、チケット付加情報保持部103から発行するチケットに適した付加情報Lを得る。

【0094】（ステップS43）チケット発行部104は、チケット特徴情報保持部102から発行したいチケットの有効期間を含むチケット特徴情報有効期間を選択する。

【0095】（ステップS44）発行したいチケットの有効期間を含むチケット特徴情報有効期間がある場合にはステップS45に進み、無い場合にはステップS46に進む。

【0096】（ステップS45）チケット発行部104は、選択したチケット特徴情報有効期間に対応するチケット秘密情報 (D, n) を入手し、そのチケット秘密情報 (D, n) と証明装置固有情報 du とチケット付加情報 L とからチケットを生成する。チケット発行は以下の式により行う。

【0097】

【数11】 $t = D - F(n, L, du)$

ここで、関数 F () は一方向性関数であり、一方向性ハッシュ関数 MD5、SHA や、共通鍵暗号 DES (Data Encryption Standard) などを用いることができる。その後、ステップS48へ進む。

【0098】（ステップS46）チケット発行部104は、発行したいチケットの有効期間を、チケット特徴情報有効期間に沿って複数の期間に分割する。

【0099】（ステップS47）分割した複数の有効期間毎に、チケット特徴情報有効期間に対応するチケット秘密情報 (D, n) を取り出し、その各チケット秘密情報 (D, n) と証明装置固有情報 du とチケット付加情報 L とから複数のチケットを生成する。

【0100】（ステップS48）チケット発行装置100は、生成したチケット t を、法数 n およびチケット付加情報 L と組にして、(t, n, L) の形式で発行する。チケットが複数ある場合は、複数の (t, n, L) をチケットとして発行する。

【0101】以下では、図9のフローチャートに沿って、利用者識別番号が003である利用者から、1997年8月10日から3ヶ月間有効な、遊園地の定期入場券の発行要求があったときのチケットの発行手順を例にして説明する。まずステップS41で、チケット発行部104は、チケット発行要求元の利用者の利用者番号を元に、第1の証明装置固有情報保持部101を検索して利用者の証明装置固有情報を検索する。いま、第1の証明装置固有情報保持部101の内容が図4に示すもので

あるとすると、利用者識別番号が003であるので、証明装置固有情報d003を検索する。

【0102】次にステップS42で、チケット付加情報Lを得る。ここでは、チケット付加情報L310は以下

チケット名称： AAA遊園地定期入場券、
有効期間： 1997年8月10日～1997年11月9日
発行場所： 横浜チケットセンター

ステップS43では、チケット特徴情報有効期間を選択する。いま、チケット特徴情報保持部102の内容が図3に示すものであるとすると、発行したいチケットの有効期間は1997年8月10日～1997年11月9日であるので、適切なチケット特徴情報有効期間が存在しない。そのため、ステップS44では、ステップS46に進む。

【0104】ステップS46では、発行したいチケットの有効期間を、チケット特徴情報有効期間に沿って複数の期間に分割する。ここでは、発行したいチケットの有効期間は1997年8月10日～1997年11月9日を、図3のチケット特徴情報有効期間に沿って、以下のように4つに分割する。

【0105】

【表3】1997年8月10日～1997年8月31日
1997年9月1日～1997年9月30日
1997年10月1日～1997年10月31日
1997年11月1日～1997年11月9日

ステップS47では、分割した複数の有効期間毎に、チケット特徴情報有効期間に対応するチケット秘密情報(D, n)を取り出し、その各チケット秘密情報(D, n)と証明装置固有情報duとチケット付加情報Lとから複数のチケットを生成する。ここでは、上記のように分割した各有効期間毎に対応するチケット秘密情報は、それぞれ(D8, n8)、(D9, n9)、(D10, n10)、(D11, n11)であるので、これらを元にして、以下の4つのチケットを作成する。

【0106】

【数12】

$t311 = D8 - F(n8, L311, d003)$

$t312 = D9 - F(n9, L312, d003)$

$t313 = D10 - F(n10, L313, d003)$

$t314 = D11 - F(n11, L314, d003)$

ここで、L311～L314は、L310の有効期間の部分各チケットにあわせて変更したものである。

【0107】ステップS48では、このようにして生成したチケットを、法数nおよびチケット付加情報Lと組にして発行する。つまり、以下の4組のチケットを発行する。

【0108】

【数13】(t311, n8, L311)

(t312, n9, L312)

(t313, n10, L313)

のような情報であるとする。

【0103】

【表2】

(t314, n11, L314)

以上のようにして発行されたチケットの組みは、利用者の証明装置200に格納される。チケットの使用の際は、第1の実施例と同様に、利用者が予め証明装置200上で使用するチケットを選択しておき、検証装置300からの認証情報に対して証明情報を返送することによって、正当な証明装置200と正当なチケットとを保持していることを証明して、入場ゲートを開いてもらう。

【0109】ここでは、上記説明したように、チケット使用の際に予め利用者が使用するチケットを選択しておくようにして説明したが、必ずしもこの方法を取らなくても構わない。例えば、検証装置300が認証情報とともに、有効公開情報選択部307により選択した現在有効な法数nを証明装置200に送り、証明装置200ではその法数nを検索キーにしてチケット保持部201から使用するチケットを選択して、証明情報を生成するという方法をとっても構わない。また、本実施例では、チケット付加情報が存在する例を用いて説明したが、たとえばチケットの種類が1種類しかなく、チケット付加情報によるチケットの区別などが必要ない場合には、チケット付加情報を含めない構成も可能である。

【0110】[第3の実施例] 第3の実施例では、法数nおよび秘密鍵Dを一定期間毎に変更するが、同時期に複数の有効な法数nおよび秘密鍵Dが存在する例について説明する。第1および第2の実施例では、法数nおよび秘密鍵Dを一斉に変更する例であり、ある時点での法数nおよび秘密鍵Dは一意に決めることができた。しかし、第3の実施例では、同時期に複数の有効な法数nおよび秘密鍵Dが存在するため、検証を行う際に、どのチケット公開情報を用いて行うかを決める必要がある。

【0111】本実施例では、チケット発行装置は、チケット特徴情報有効期間の一部期間が重複するように決められた法数nと秘密鍵Dのリストを有し、それを用いて発行を要求された日時のチケットを作成する。

【0112】定期券、回数券などの場合には、定期券、回数券などの有効期間が、チケット特徴情報有効期間内に収まるように発行する。収まるような期間がない場合には、分割して発行する。

【0113】以下では、同時期に複数の有効な法数nと秘密鍵Dが存在し、検証装置側から複数の有効な法数を用いて認証情報を複数回送る例について説明する。

【0114】図10は第3の実施例の構成図である。図10において、電子チケットシステムは、第1の実施例

と同様にチケット発行装置 1 0 0、証明装置 2 0 0、検証装置 3 0 0 を含んで構成されている。各装置の内容も第 1 の実施例と似ている。以下では異なる部分を中心に説明する。

【0 1 1 5】チケット発行装置 1 0 0 は、第 1 の実施例と同様に第 1 の証明装置固有情報保持部 1 0 1 と、チケット特徴情報保持部 1 0 2 と、チケット付加情報保持部 1 0 3 と、チケット発行部 1 0 4 とから構成される。このうち、第 1 の証明装置固有情報保持部 1 0 1 とチケット付加情報保持部 1 0 3 は第 1 の実施例と同様である。

【0 1 1 6】チケット特徴情報保持部 1 0 2 は、チケットを発行する際に用いるチケット秘密情報を保持するもので、発行するチケットの有効期間にあわせて選択できるように、チケット秘密情報の有効期間を表すチケット特徴情報有効期間とチケット秘密情報とに加えてチケット特徴情報識別子に対応させて保持している。第 1 の実施例では、このチケット特徴情報有効期間は重複することがないように構成されていたが、本実施例では、一部重複するように構成されている。本実施例におけるチケット特徴情報保持部 1 0 2 に保持されている情報の例を図 1 1 に示す。この図では、4 ヶ月毎に 1 つのチケット特徴情報に対応しており、それが 1 ヶ月毎に変更されるようになっている。

【0 1 1 7】チケット発行部 1 0 4 は、第 1 の実施例と同様に、利用者から要求されたチケットを生成する部分であり、発行を要求した利用者の証明装置固有情報と、チケットの有効日または有効期間にあわせて選択されたチケット秘密情報と、チケット付加情報とからチケットを生成する。

【0 1 1 8】証明装置 2 0 0 は、各構成部分に保持される内容の構成が少し異なるだけで、基本的な機能は第 1 の実施例と同様である。証明装置 2 0 0 の証明情報生成部 2 0 3 は、認証情報入力部 2 0 2 に入力された認証情報を元にして、対応するチケット、証明装置固有情報とを用いて証明情報を生成し、検証装置 3 0 0 へ送る。対応するチケットは、認証情報に添付されて送られてくる法数を検索キーにして、チケット保持部 2 0 1 から検索する。適切なチケットの検索に成功すると、証明情報生成部 2 0 3 は正しい証明情報を生成し、チケットの検索に失敗すると正しい証明情報を生成しない。ここでいう正しい証明情報を生成しないとは、例えば証明情報として、“0”などの値を生成することである。このようにして生成した証明情報を、検証装置 3 0 0 に送る。

【0 1 1 9】検証装置 3 0 0 の構成要素は第 1 の実施例と同様であるが、各構成要素の関係が少し異なる。

名称： 定期券、
区間： 東京－横浜、
有効期間： 1 9 9 7 年 8 月 1 0 日～1 9 9 7 年 1 1 月 9 日
発行場所： 横浜チケットセンター

ステップ S 5 3 で、図 1 1 に示すチケット特徴情報保持

【0 1 2 0】チケット公開情報保持部 3 0 6 は、チケット発行装置 1 0 0 のチケット特徴情報保持部 1 0 2 に対応して、チケット特徴情報有効期間の保持の仕方が変わっている。チケット公開情報保持部 3 0 6 は、チケット特徴情報有効期間とチケットの公開情報との組からなる有効期限付きチケット公開情報を保持する部分である。チケット特徴情報有効期間は、チケット発行装置 1 0 0 のチケット特徴情報保持部 1 0 2 が保持しているチケット特徴情報有効期間と同じ物で、同じチケット特徴情報有効期間に対応するチケット秘密情報とチケット公開情報とが対応している。第 1 の実施例では、このチケット特徴情報有効期間は重複することがないように構成されていたが、本実施例では、一部重複するように構成されている。本実施例におけるチケット公開情報保持部 3 0 6 の情報の例を図 1 2 に示す。この図では、4 ヶ月毎に 1 つのチケット特徴情報に対応しており、それが 1 ヶ月毎に変更されるようになっている。

【0 1 2 1】有効公開情報選択部 3 0 7 は、現時点で有効なチケット公開情報を複数選択する部分であり、チケット公開情報の選択には、利用時の日時と、チケット公開情報保持部のチケット特徴情報有効期間とを対比させて、適切な情報を複数選択する。

【0 1 2 2】認証情報生成部 3 0 1 は、証明装置 2 0 0 との間で対話して正当なチケットを保持していることを検証するための認証情報を生成する部分であり、リプレイ攻撃を防ぐために乱数などを用いて生成することが望ましい。認証情報生成部 3 0 1 は、乱数を用いて生成した認証情報に、有効公開情報選択部 3 0 7 で選択した複数のチケット公開情報中の法数を添付したものを複数個生成し、複数回、証明装置 2 0 0 に送る。

【0 1 2 3】対話検証部 3 0 4 は、認証情報に応答して証明装置 2 0 0 から送られてきた証明情報に対して、その都度検証を行う。そして、検証に成功すれば、サービス提供部 3 0 8 からサービスを提供する。

【0 1 2 4】図 1 3 に第 3 の実施例におけるチケット発行装置 1 0 0 のフローチャートを示す。図 1 3 を元に、利用者識別番号が 0 0 3 である利用者から、1 9 9 7 年 8 月 1 0 日から 3 ヶ月間有効な定期券の発行要求があったときの例について簡単に説明する。

【0 1 2 5】ステップ S 5 1 および S 5 2 で、証明装置固有情報 d 0 0 3 と、チケット付加情報 L 3 3 1 が選ばれる。チケット付加情報 L 3 3 1 は以下のような内容である。

【0 1 2 6】

【表 4】

部 1 0 2 から適切なチケット特徴情報有効期間を選ぶ

と、適切なチケット特徴情報有効期間は1つだけあるので、ステップS54、ステップS55、ステップS57と進み、ステップS57で、チケット秘密情報(D8, n8)と、チケット特徴情報識別子n-id8と、証明装置固有情報d003と、チケット付加情報L331とを用いて、以下のチケットを生成する。

【0127】

【数14】

$t331 = D8 - F(n8, L331, d003)$

そして、ステップS60で、法数nおよびチケット付加情報Lと組にして発行する。

【0128】

【数15】 ($t331, n8, L331, n-id8$)

次に、このようにして発行されたチケットを保持する利用者が、1997年9月9日に改札を通ろうとしたときを例にして、第3の実施例における検証装置300と証明装置200の処理の流れを具体的に示す。第3の実施例における証明装置200と検証装置300の処理のフローチャートをそれぞれ図14、図15に示す。

【0129】証明装置200は、上記で発行されたチケット($t331, n8, L331, n-id8$)を、そのチケット保持部に保持しているものとする。

【0130】まず、利用者が証明装置200を改札機に挿入すると、改札機の検証装置300が起動する。以下、図15に沿って説明する。

【0131】図15のステップS81で、検証装置300の有効公開情報選択部307は、時計から現在の日時である1997年9月9日を入力し、それを元にチケット公開情報保持部306から、現在有効なチケット公開情報を複数個選択する。いま、チケット公開情報保持部306の内容は図12に示すようになっているので、このチケット特徴情報有効期間の中から1997年9月9日を含むものをすべて取り出す。その結果、対応するチケット公開情報として、以下の3組が選択される。

【0132】

【数16】 ($E7, n7$)

($E8, n8$)

($E9, n9$)

ステップS82、ステップS83およびステップS84で、まず、一番上のチケット公開情報($E7, n7$)を選択して、認証情報(C1, n7)を生成し、認証情報保持部302に保持するとともに、証明装置200に送る。

【0133】認証情報(C1, n7)を送られた証明装置200では、図4に示すように、法数n7を検索キーにしてチケット保持部201を検索するが(ステップS71~S73)、対応するチケットが保持されていないので、検索に失敗して、その結果、証明情報として

【0134】

【数17】 $R=0$

を返す(ステップS74、S75、S77)。

【0135】図15のステップS85およびステップS86で、検証装置300の対話検証部304は、この証明情報Rと、認証情報(C1, n7)と、チケット公開情報($E7, n7$)を用いて検証を行うが、検証に失敗し、ステップS82へ戻る。

【0136】次に、ステップS82、ステップS83およびステップS84で、2番目のチケット公開情報($E8, n8$)を選択して、認証情報(C2, n8)を生成し、認証情報保持部302に保持するとともに、証明装置200に送る。

【0137】認証情報(C2, n8)を送られた証明装置200では、図4に示すように、法数n8を検索キーにしてチケット保持部を検索し(ステップS73)、

【0138】

【数18】 ($t331, n8, L331, n-id8$)
の検索に成功して、このチケットを用いて、証明情報

【0139】

【数19】

$R = C2^{t331} C2^{F(n8, L331, d003)} \bmod n8$

を検証装置300に返送する(ステップS74、S76、S77)。

【0140】図15のステップS85およびステップS86で、検証装置300の対話検証部304は、この証明情報Rと、認証情報(C2, n8)と、チケット公開情報($E8, n8$)を用いて検証を行う。検証は、以下の式に基づいて行い、検証に成功する。

【0141】

【数20】

$R^{E8} = (C2^{t331} C2^{F(n8, L331, d003)})^{E8}$

$\equiv C2^{D8E8}$

$\equiv C2 \pmod{n}$

ステップS87に進み、利用者にサービスを提供する。具体的には、改札のゲートをあけて、利用者が中に入るようにする。

【0142】第3の実施例では、法数nおよび秘密鍵Dを一定期間毎に変更するが、同時期に複数の有効な法数nおよび秘密鍵Dが存在する例について説明した。第1および第2の実施例のように法数nおよび秘密鍵Dを一斉に変更する例に比べて、万一秘密鍵Dが漏洩したとしても、即座に秘密鍵Dを変更することが可能になる。すでに発行してしまったチケットを無効にしない場合には、検証装置300では漏洩した秘密鍵による検証を行う必要があるが、チケット発行装置100では、漏洩した秘密鍵Dによるチケットの発行を即座に中止することが可能になり、被害の拡大を防ぐことができる。

【0143】また、本実施例では、検証装置300から証明装置200に認証情報を送る際に、法数nを添付して送るようにして説明したが、この法数nのかわりにチケット特徴情報識別子n-idを添付して送るように構

成しても構わない。一般に法数 n は数百～数千ビットの大きな数字であるので法数を送るときには通信に時間がかかるが、チケット特徴情報識別子 $n-id$ は数ビットから数十ビット程度で済むので、通信時間が少なくて済む

【0144】[第4の実施例]

(例) 第4の実施例では、第3の実施例と同様に、法数 n および秘密鍵 D を一定期間毎に変更するが、同時期に複数の有効な法数 n および秘密鍵 D が存在する例について説明する。本実施例では、チケット発行装置100は

【0145】本実施例では、回数券などのような、同じチケットを用いてある期間中に有限回の検証が可能なチケットについて説明する。この例では、同時期に複数の有効なチケット特徴情報が存在し、認証情報に対して証明装置200側から法数を送るようになっている。

【0146】第4の実施例の構成図を図16に示す。図16において、チケット発行装置100は、第3の実施例と同じである。検証装置300の構成は、第1の実施

名称： 回数券、
区間： 東京ー横浜、
利用可能回数： 11回
有効期間： 1997年8月10日～1997年11月9日
発行場所： 横浜チケットセンター

このようなチケットを証明装置200のチケット保持部201に格納する際に、本実施例では証明装置200の内部状態の初期化を行う。証明装置200の内部状態は、各チケットに1対1で対応するように内部状態を持つ。チケットをチケット保持部201に格納する際には、まず以前にそのチケットが格納されたことがないかどうかを確認した上で、初めてのチケットの場合にのみ、対応する内部状態を確保する。以前にチケットが格納されたかどうかを判断するためには、各チケット毎にチケット id のようなものを持たせて、それで管理すればよい。ここでは、各チケット $t341$ の添え字にあたる部分(341の部分)をチケット id として扱えばよい。このようにして各チケットに1対1で対応するように内部状態を確保した上で、初期化時には”0”を書き込む。これは回数券の利用回数を書き込むためのものであり、チケットを利用する度に1ずつカウントアップしていき、チケット付加情報の利用可能回数に達したら、それ以上の利用を中止させるのに用いる。

【0150】上記のチケット $t341$ を証明装置200のチケット保持部201に格納したときの、内部状態保持部205の内容の例を図19に示す。チケット保持部201には、さまざまなチケットが格納されており、その中で内部状態を必要とする回数券にのみ内部状態が確保され、初期値”0”が書き込まれている。ここでは回数券の例を説明するために、回数券にのみ内部状態を持

例と同じである。証明装置200は、チケット保持部201、認証情報入力部202、証明情報生成部203、第2の証明装置固有情報保持部204に加えて、内部状態保持部205を有している。この例では、内部状態保持部205は、各チケット毎にチケットの使用回数をカウントし、そのカウント数を保持するものである。

【0147】本実施例では、1997年8月10日から3ヶ月間有効な回数券を1997年9月9日に使用する場合について、簡単に説明する。回数券の利用可能回数は11回であるとする。利用者の利用者識別番号が003であるとする、以下のようなチケットが発行される。発行の手順は第3の実施例と同様である。

【0148】

【数21】($t341, n8, L341, n-id8$)
 $t341 = D8 - F(n8, L341, d003)$
ここで、チケット付加情報 $L341$ は、以下の情報である。

【0149】

【表5】

たせるようにして、内部状態としては回数を表す数字の例で示したが、内部状態はこれに限ることはない。たとえば、鉄道の切符の入札済みや出札済みなどの状態や、どこの駅から乗車したかを記録したり、総利用時間の制限のあるチケットの場合には現在までの利用時間を記録したり、あるいはある航空会社の飛行機に乗ったマイル数を積算したりなどの用途に用いることができる。

【0151】以下では、証明装置200は、上記のようにして格納されたチケットをチケット保持部201に保持し、図19に示す内部状態になっているものとして、図17に沿って、証明装置200の処理を説明する。

【0152】図17において、証明装置200は、検証装置300から認証情報 C を受け、第2の証明装置固有情報保持部から証明装置固有情報 $d003$ を取得し、チケット保持部からチケット($t341, n8, L341, n-id8$)を取得する(ステップS91～S93)。

【0153】次に証明装置200は、内部状態を読み出し、チケット付加情報の利用可能回数と比較する(S94)。いま、内部状態は”0”であり、チケット付加情報の利用可能回数は11回であるので、利用可能であると判定して、内部状態を1だけ増加させて1にし、証明情報を生成する(S95、S96)。

【0154】

【数22】

$$R = C^{t341} C^F(n8, L341, d003) \bmod n8$$

一方もし、内部状態が”11”であるときには、その回数券の利用可能回数まで使用し終わっているの、利用不可と判定し、証明情報 $R=0$ とする(S97)。

【0155】証明装置200は、このようにして生成した証明情報に、チケット特徴情報識別子 $n-id8$ を付加して($R, n-id8$)として、検証装置300に送る(S98)。

【0156】以上で証明装置200の説明は終わりである。

【0157】次に、図18に沿って検証装置300の処理を説明する。

【0158】図18において、まず、検証装置300は、認証情報 C を生成し、認証情報保持部302に保持するとともに、証明装置200に送る(S101)。

【0159】次に、検証装置300の有効公開情報選択部307は、時計305から現在の日時である1997年9月9日入手し、それを元にチケット公開情報保持部306から、現在有効なチケット公開情報を複数個選択する(S102)。いま、チケット公開情報保持部306の内容は図12に示すようになっているので、このチケット特徴情報有効期間の中から1997年9月9日を含むものをすべて取り出す。その結果、対応するチケット公開情報として、以下の3組が選択される。

【0160】

【数23】($E7, n7, n-id7$)

($E8, n8, n-id8$)

($E9, n9, n-id9$)

次に対話検証部304は、証明装置200から送られてきた証明情報($R, n-id8$)のチケット特徴情報識別子 $n-id$ を検索キーにして、上記3組のチケット公開情報を検索する(S103)。その結果、チケット公開情報($E8, n8, n-id8$)が検索される。ここで、このような検索を行っているのは、証明装置200から送られてきた証明情報が現在有効なチケット公開情報に基づいて作成されているかどうかを確認するためである。この確認を行わないと、証明情報にチケット特徴情報識別子 $n-id$ のかわりに、法数 n そのものを用いた場合に、公開情報 E に対応する不正な秘密情報 D と不正な法数 n との組を作成されれば、不正に証明情報を作成することが可能になってしまう。この例では、検索は成功したので、証明装置200から送られてきた証明情報が現在有効なチケット公開情報に基づいて作成されていることが確認された。

【0161】次に、検証装置300は、証明情報($R, n-id8$)と、認証情報 C と、チケット公開情報($E8, n8, n-id8$)とを用いて検証を行う(S105)。検証は、以下の式に基づいて行い、検証に成功する。

【0162】

【数24】

$$R^{E8} \equiv (C^{t341} C^F(n8, L341, d003))^{E8}$$

$$\equiv C^{D8E8}$$

$$\equiv C \pmod{n}$$

検証に成功したので、検証装置は利用者にサービスを提供する(S106、S107)。ここでは、改札のゲートを開けて、利用者が中に入れるようにする。なお、チケット公開情報の検索に失敗したり、検証に失敗した場合には、認証失敗処理を行なう(S108)。

10 【0163】本実施例では、証明装置200が認証情報を受けて、チケット付加情報等と照らし合わせた上で、内部状態の変更を行っている。この例では、証明装置200が検証装置300の正当性を検証していないので、万一不正な検証装置300があった場合には、不正に内部状態の変更を許してしまう。これを避けるためには、証明装置200が検証装置300から認証情報を受け取って、チケット付加情報等と照らし合わせた後に、今度は逆に証明装置200が第2の認証情報を作成して検証装置300に送り、検証装置300がその第2の認証情報を元にして第2の証明情報を生成して証明装置200に送り返し、証明装置200はその第2の証明情報を検証して、検証装置300の正当性を確認した上で、内部状態を変更して、最初の認証情報に対する証明情報を生成して、検証装置300に送るといった構成にすればよい。

【0164】また、上述したように、ここでは回数券の例を説明するために、回数券にのみ内部状態を持たせるようにして、内部状態としては回数を表す数字の例で示したが、内部状態はこれに限ることはない。たとえば、鉄道の切符の入札済みや出札済みなどの状態を記録するために、入札済みや出札済みなどの状態を表す情報を記録したり、どの駅から乗車したかを記録したり、総利用時間の制限のあるチケットの場合には現在までの利用時間を記録したり、あるいはある航空会社の飛行機に乗ったマイル数を積算して記録したりなどの用途に用いることができる。

【0165】さらに、証明装置200の内部状態は、各チケットに1対1で対応するように内部状態を持つように説明したが、これもこの方法に限ることはない。例えば、ある回数券が2枚に分割されて発行されている場合などには、発行された2枚の回数券に対して1つの内部状態を持つように構成することで、1枚目の回数券を使用した利用回数を、2枚目の回数券の利用回数に引き継ぐことが可能になる。このように、ある回数券が2枚に分割されて発行されている場合には、別の方法として、内部状態は2つ持たせて、どちらの回数券を利用したときでも、両方の内部状態を同時に変更するというような構成にしても構わない。

50 【0166】[第5の実施例] 第5の実施例では、RSA暗号ではなく、離散対数系の暗号方式を用いる。この

例においては、同時期に複数の有効なチケット特徴情報が存在し、通信路上には法数は流れず検証装置が認証情報を複数回検証するようになっている。チケットの特徴情報は以下の形で与えられる。

【0167】 p は素数であり、 G は離散対数問題が困難な有限群であり、 g は有限群 G の位数 p の元であり、

【0168】

$$【数25】 y = g^x \mod p$$

が満たされるとき、 (p, G, g, y, x) がチケットの特徴情報である。特に (p, G, g, y) を公開の特

徴情報とし、 x を秘密の特徴情報とする。

【0169】実際には、 G を有限体の乗法群として構成したり、有限体上の楕円曲線として構成することができる。

【0170】本実施例では、 (G, g) をシステム共通とし、公開情報 (y, p) 、秘密情報 x とすると、チケットは

【0171】

$$【数26】 t = x - F(y, L, du)$$

として構成することができる。ここで、関数 F や L や du などは、RSAの例の場合と同様である。

名称： 定期券、

区間： 東京ー横浜、

有効期間： 1997年8月10日～1997年11月9日

発行場所： 横浜チケットセンター

ステップS113で、図22に示すチケット特徴情報保持部102から適切なチケット特徴情報有効期間を選ぶと、適切なチケット特徴情報有効期間は1つだけあるので、ステップS114、ステップS115、ステップS117と進み、ステップS117で、チケット秘密情報 x_8 とチケット公開情報 (y_8, p_8) と証明装置固有情報 $d003$ とチケット付加情報 $L351$ とを用いて、以下のチケットを生成する。

【0176】

【数27】

$$t351 = x_8 - F(y_8, L351, d003)$$

そして、ステップS120で、 (y, p) およびチケット付加情報 L と組にして発行する。

【0177】

【数28】 $(t351, y_8, p_8, L351)$

次に、このようにして発行されたチケットを保持する利用者が、1997年9月9日に改札を通ろうとしたときを例にして、第5の実施例における検証装置300と証明装置200の処理の流れを具体的に示す。第5の実施例における証明装置200と検証装置300の処理のフローチャートをそれぞれ図24、図25に示す。

【0178】まず証明装置200について図24に基づいて説明する。図24において、まず、証明装置200は、検証装置300から認証情報 C を受け取る(S131)。次に、証明情報生成部203は、チケット保持部

【0172】第5の実施例の構成図を図20に示す。構成は第4の実施例とほぼ同様であり、図16とほぼ同様である。ただし本実施例では、チケット発行装置100のチケット特徴情報保持部102は、チケット特徴情報有効期間とチケット秘密情報とに加えて、チケット公開情報も対応させて保持している。そしてチケット発行部104は、証明装置固有情報とチケット秘密情報とチケット付加情報とに加えて、チケット公開情報とからチケットを生成する。

【0173】第5の実施例のチケット発行装置のフローチャートを図21に示す。第3の実施例と同じように、利用者識別番号が003である利用者から、1997年8月10日から3ヶ月間有効な定期券の発行要求があったときの例について簡単に説明する。

【0174】ステップS111およびS112で、証明装置固有情報 $d003$ と、チケット付加情報 $L351$ が選ばれる。チケット付加情報 $L351$ は以下のような内容である。

【0175】

【表6】

201からチケット $(t351, y_8, p_8, L351)$ を取得し、第2の証明装置固有情報保持部204から証明装置固有情報 $d003$ を取得する(S132)。そして、これらの情報に基づいて証明情報 R を生成して、検証装置300に送る(S133)。証明情報 R の計算式は以下の通りである。

【0179】

【数29】

$$R = C^{t351} \cdot C^{F(y_8, L351, d003)} \mod p_8$$

次に、検証装置300について図25に基づいて説明する。図25において、利用者が証明装置200を改札機に挿入すると、改札機の検証装置300が起動する。

【0180】ステップS141で、検証装置300は、乱数 r を生成し、この乱数を用いて認証情報 C を以下の式により生成し、認証情報保持部302に保持するとともに、証明装置200に送る。

【0181】

$$【数30】 C = g^r \mod p$$

ただし、 r は乱数

次に、ステップS142で、検証装置300の有効公開情報選択部307は、時計から現在の日時である1997年9月9日を入力し、それを元にチケット公開情報保持部306から、現在有効なチケット公開情報を複数個選択する。いま、チケット公開情報保持部306の内容は図23に示すようになっているので、このチケット特

傲情報有効期間の中から1997年9月9日を含むものをすべて取り出す。その結果、対応するチケット公開情報として、以下の3組が選択される。

【0182】

【数31】 (y7, p7)

(y8, p8)

(y9, p9)

次に、ステップS143、ステップS144へと進み、

まず、一番上のチケット公開情報 (y7, p7) を取り

$$\begin{aligned} R &= C^{t351} C^F(y8, L351, d003) \bmod p8 \\ &= C^{x8-F(y8, L351, d003)} C^F(y8, L351, d003) \bmod p8 \\ &= C^{x8} \bmod p8 \\ &= (g^r)^{x8} \bmod p8 \\ &= g^{rx8} \bmod p8 \end{aligned}$$

一方、公開情報 y は以下の式により与えられている。

【0186】

【数34】 $y = g^x \bmod p$

そのため、 y^r の値は以下になる。

【0187】

$$g^{rx} \bmod p = ? \quad g^{rx8} \bmod p8 \quad (a)$$

さて、チケット公開情報が (y7, p7) の時には、上の式は成り立たない。検証に失敗したので、ステップS146からステップS143へ戻り、ステップS144へ進んで、2番目のチケット公開情報 (y8, p8) を取り出す。

【0189】ステップS145で、このチケット公開情報 (y8, p8) と、証明情報 R と、認証情報 C とを用いて検証を行う。(a) 式を用いて検証を行うと、

(a) 式は成り立つ。

【0190】これで検証は成功したので、ステップS147へ進み、利用者へサービスを提供する。具体的には、改札のゲートをあけて、利用者が中に入れるようにする。

【0191】

【発明の効果】以上説明したように、この発明によれば、証明装置および検証装置において有効期間に応じた証明用の情報および検証用の情報を選択して対話証明を行なうようにして、有効期間ごとに秘密情報が異なるようにできるようにしている。したがって、チケット秘密情報に有効期間を設けることができ、チケット秘密情報 40 が露呈した場合でも、被害を少なく押さえることができる。

【図面の簡単な説明】

【図1】 第1の実施例における電子チケットシステムの構成を示すブロック図である。

【図2】 図1におけるデータの流れを説明するブロック図である。

【図3】 第1の実施例におけるチケット特徴情報保持部の内容の例を説明する図である。

【図4】 第1の実施例における第1の証明装置固有情 50

出す。

【0183】ステップS145で、このチケット公開情報 (y7, p7) と、証明情報 R と、認証情報 C とを用いて検証を行う。検証には、以下の式を用いる。

【0184】

【数32】 $y^r \equiv ? \quad R \bmod p$

いま、証明情報 R は以下のようにになっている。

【0185】

【数33】

$$\begin{aligned} \text{【数35】 } y^r &\equiv g^{rx} \bmod p \\ \text{つまり、検証には、以下の式が成り立つかどうかを計算} \\ \text{すればよい。} \end{aligned}$$

【0188】

【数36】

報保持部の内容の例を説明する図である。

【図5】 第1の実施例のチケット発行装置の処理の流れを説明するフローチャートである。

【図6】 第1の実施例の証明装置の処理の流れを説明するフローチャートである。

【図7】 第1の実施例の検証装置の処理の流れを説明するフローチャートである。

【図8】 第1の実施例の検証装置のチケット公開情報保持部の内容の例を説明する図である。

【図9】 第2の実施例のチケット発行装置の処理の流れを説明するフローチャートである。

【図10】 第3の実施例の構成を示すブロック図である。

【図11】 第3の実施例におけるチケット特徴情報保持部の内容の例を示す図である。

【図12】 第3の実施例の検証装置のチケット公開情報保持部の内容の例を示す図である。

【図13】 第3の実施例のチケット発行装置の処理の流れを説明するフローチャートである。

【図14】 第3の実施例の証明装置の処理の流れを説明するフローチャートである。

【図15】 第3の実施例の検証装置の処理の流れを説明するフローチャートである。

【図16】 第4の実施例の構成を示すブロック図である。

【図17】 第4の実施例の証明装置の処理の流れを説明するフローチャートである。

【図18】 第4の実施例の検証装置の処理の流れを説明するフローチャートである。

【図19】 第4の実施例における証明装置内の内部状

態保持部の内容の例を示す図である。

【図 2 0】 第 5 の実施例の構成を示すブロック図である。

【図 2 1】 第 5 の実施例のチケット発行装置の処理の流れを説明するフローチャートである。

【図 2 2】 第 5 の実施例におけるチケット特徴情報保持部の内容の例を示す図である。

【図 2 3】 第 5 の実施例の検証装置のチケット公開情報保持部の内容の例を示す図である。

【図 2 4】 第 5 の実施例の証明装置の処理の流れを説明するフローチャートである。

【図 2 5】 第 5 の実施例の検証装置の処理の流れを説明するフローチャートである。

【符号の説明】

- 1 0 0 チケット発行装置
1 0 1 第 1 の証明装置固有情報保持部
1 0 2 チケット特徴情報保持部

【図 3】

チケット特徴情報有効期間 (term)	チケット秘密情報 (D)	法数 (n)
...
1997.7.1~1997.7.31	D7	n7
1997.8.1~1997.8.31	D8	n8
1997.9.1~1997.9.30	D9	n9
1997.10.1~1997.10.31	D10	n10
1997.11.1~1997.11.30	D11	n11
1997.12.1~1997.12.31	D12	n12
...
...

第 1 の実施例におけるチケット特徴情報保持部の例

【図 8】

チケット特徴情報有効期間 (term)	チケット公開情報 (E)	法数 (n)
...
1997.7.1~1997.7.31	E7	n7
1997.8.1~1997.8.31	E8	n8
1997.9.1~1997.9.30	E9	n9
1997.10.1~1997.10.31	E10	n10
1997.11.1~1997.11.30	E11	n11
1997.12.1~1997.12.31	E12	n12
...
...

第 1 の実施例の検証装置のチケット公開情報保持部の例

- 1 0 3 チケット付加情報保持部
1 0 4 チケット発行部
2 0 0 証明装置
2 0 1 チケット保持部
2 0 2 認証情報入力部
2 0 3 証明情報生成部
2 0 4 第 2 の証明装置固有情報保持部
2 0 5 内部状態保持部
3 0 0 検証装置
3 0 1 認証情報生成部
3 0 2 認証情報保持部
3 0 3 証明情報保持部
3 0 4 対話検証部
3 0 5 時計
3 0 6 チケット公開情報保持部
3 0 7 有効公開情報選択部
3 0 8 サービス提供部

【図 4】

利用者識別番号(u)	証明装置固有情報(du)
...	...
001	d001
002	d002
003	d003
...	...

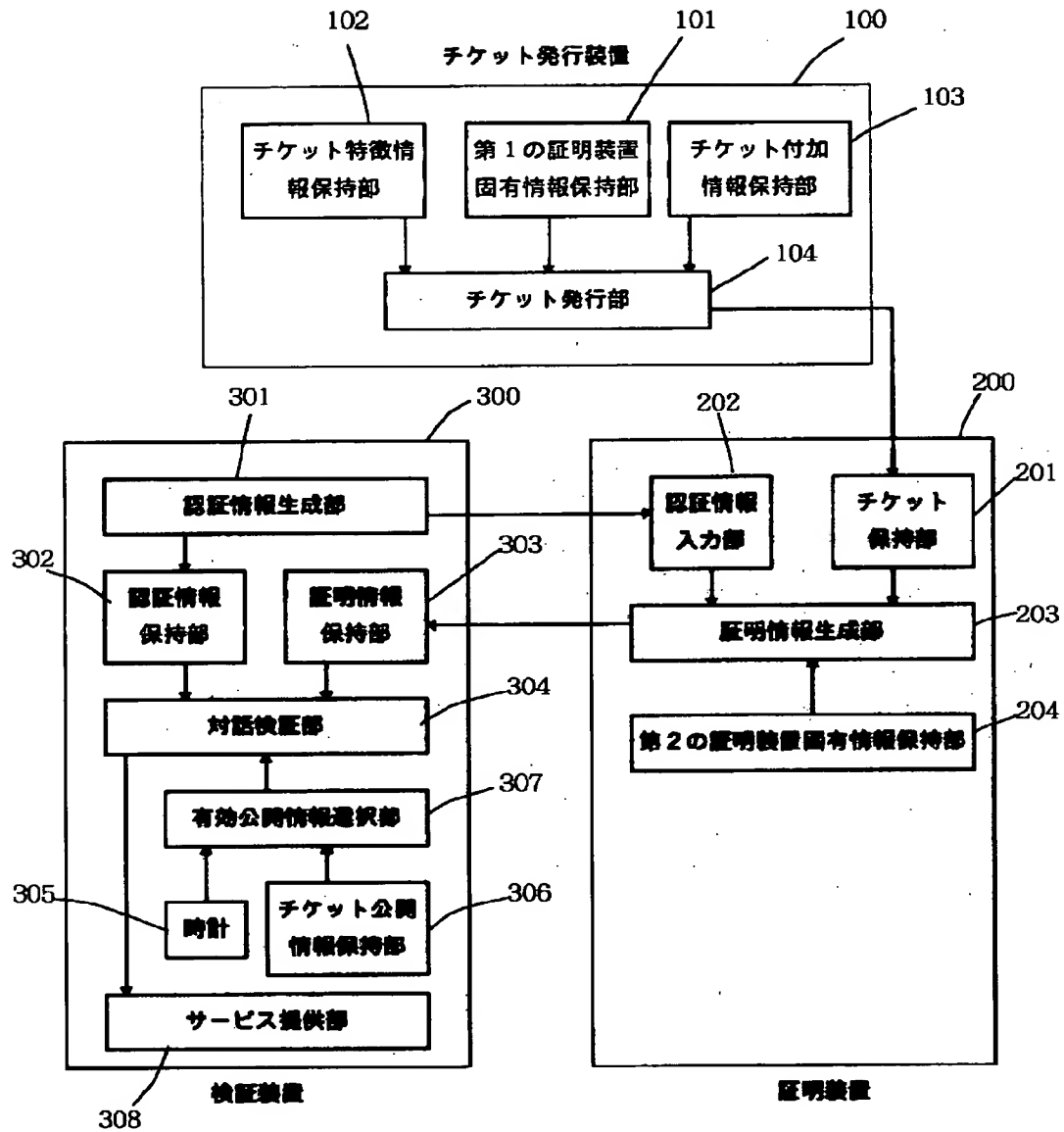
第 1 の実施例における第 1 の証明装置固有情報保持部の例

【図 1 1】

チケット特徴情報有効期間 (term)	チケット秘密情報 (D)	法数 (n)	チケット特徴情報識別子 (td)
...
1997.7.1~1997.10.31	D7	n7	n-td7
1997.8.1~1997.11.30	D8	n8	n-td8
1997.9.1~1997.12.31	D9	n9	n-td9
1997.10.1~1998.1.31	D10	n10	n-td10
1997.11.1~1998.2.28	D11	n11	n-td11
1997.12.1~1998.3.31	D12	n12	n-td12
...
...

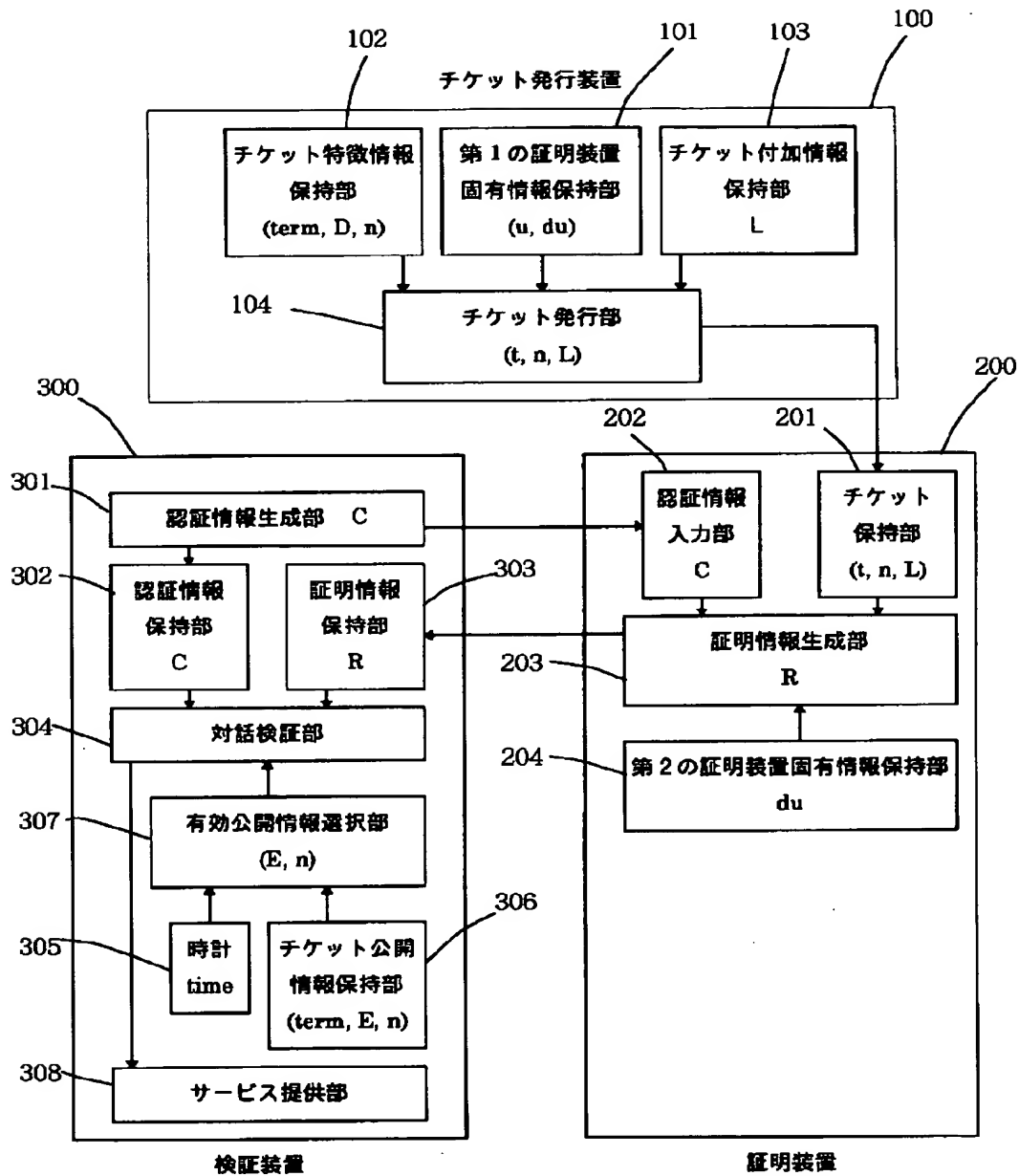
第 3 の実施例におけるチケット特徴情報保持部の例

【図1】



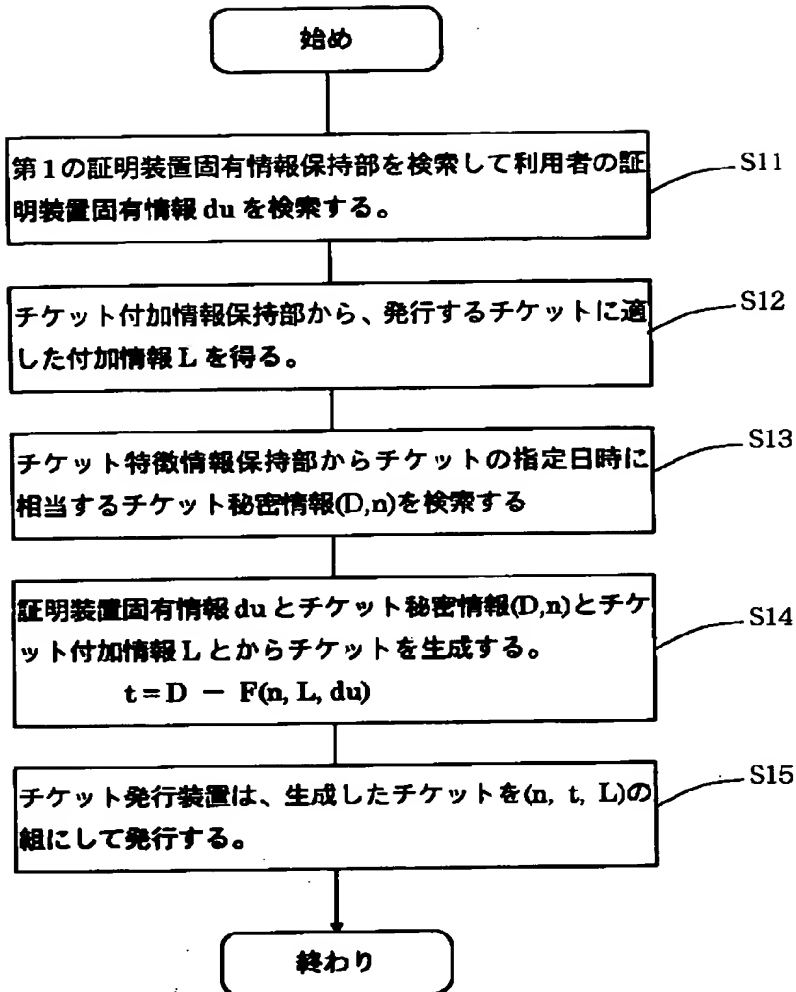
第1の実施例における電子チケットシステムの構成

【図2】



第1の実施例における電子チケットの構成（記号入り）

【図 5】



【図 19】

チケット id (i-id)	チケットの種類	内部状態
...
801	コンサートチケット	—
312	道園地入場券	—
331	定期券	—
341	回数券	0
...
...
...

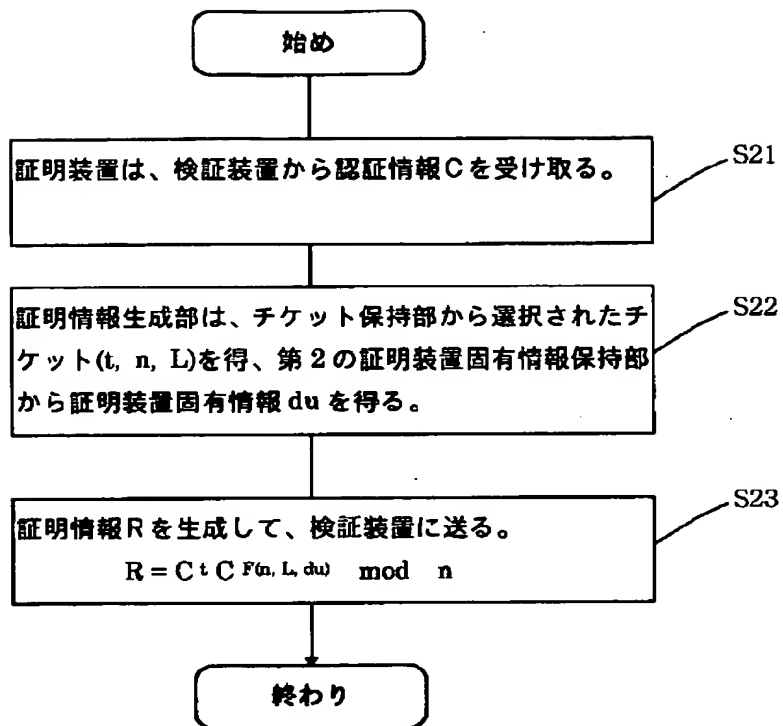
第 4 の実施例における証明装置内の内部状態保持部の例

【図 12】

チケット特徴情報有効期間 (term)	チケット公開情報 (E)	法数 (n)	チケット特徴情報識別子 (id)
...
1997.7.1~1997.10.31	E7	n7	n-id7
1997.8.1~1997.11.30	E8	n8	n-id8
1997.9.1~1997.12.31	E9	n9	n-id9
1997.10.1~1998.1.31	E10	n10	n-id10
1997.11.1~1998.2.28	E11	n11	n-id11
1997.12.1~1998.3.31	E12	n12	n-id12
...
...

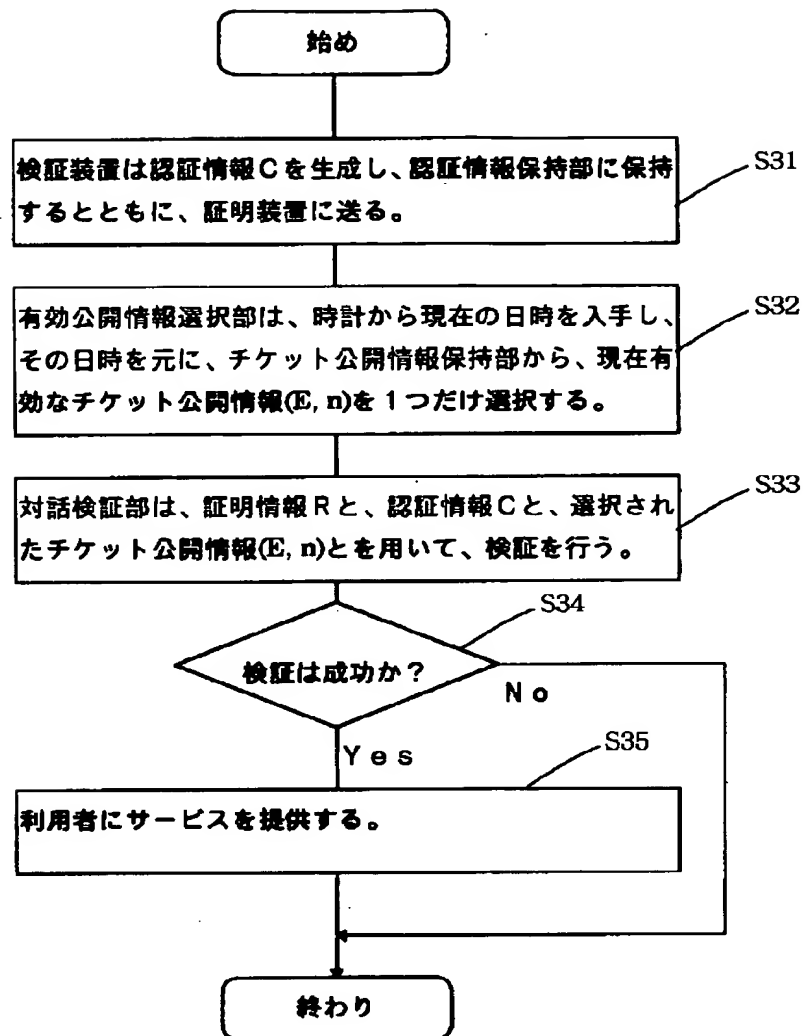
第 8 の実施例の検査装置のチケット公開情報保持部の例

【図 6】



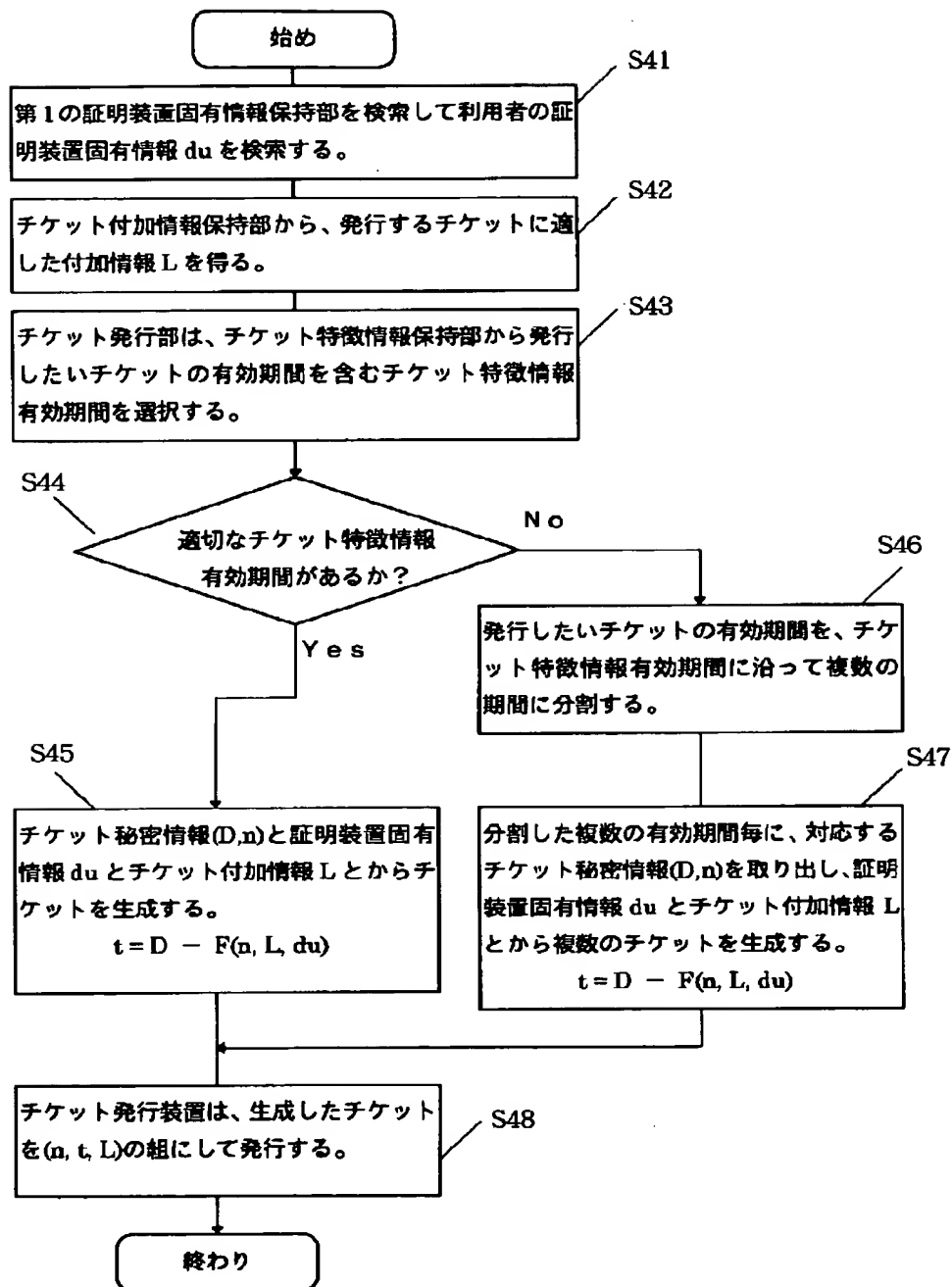
第 1 の実施例の証明装置の処理の流れ

【図7】



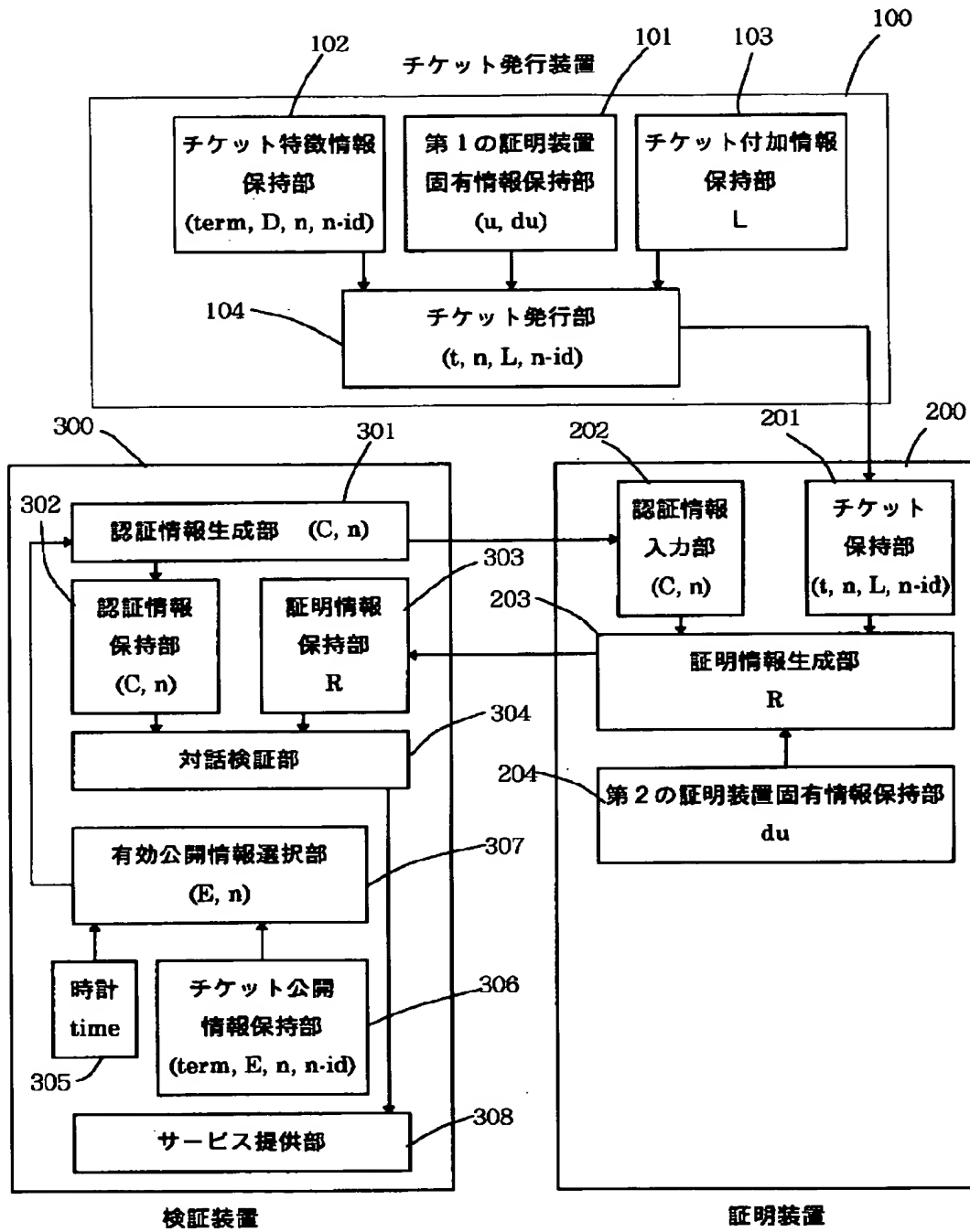
第1の実施例の検証装置の処理の流れ

【図 9】



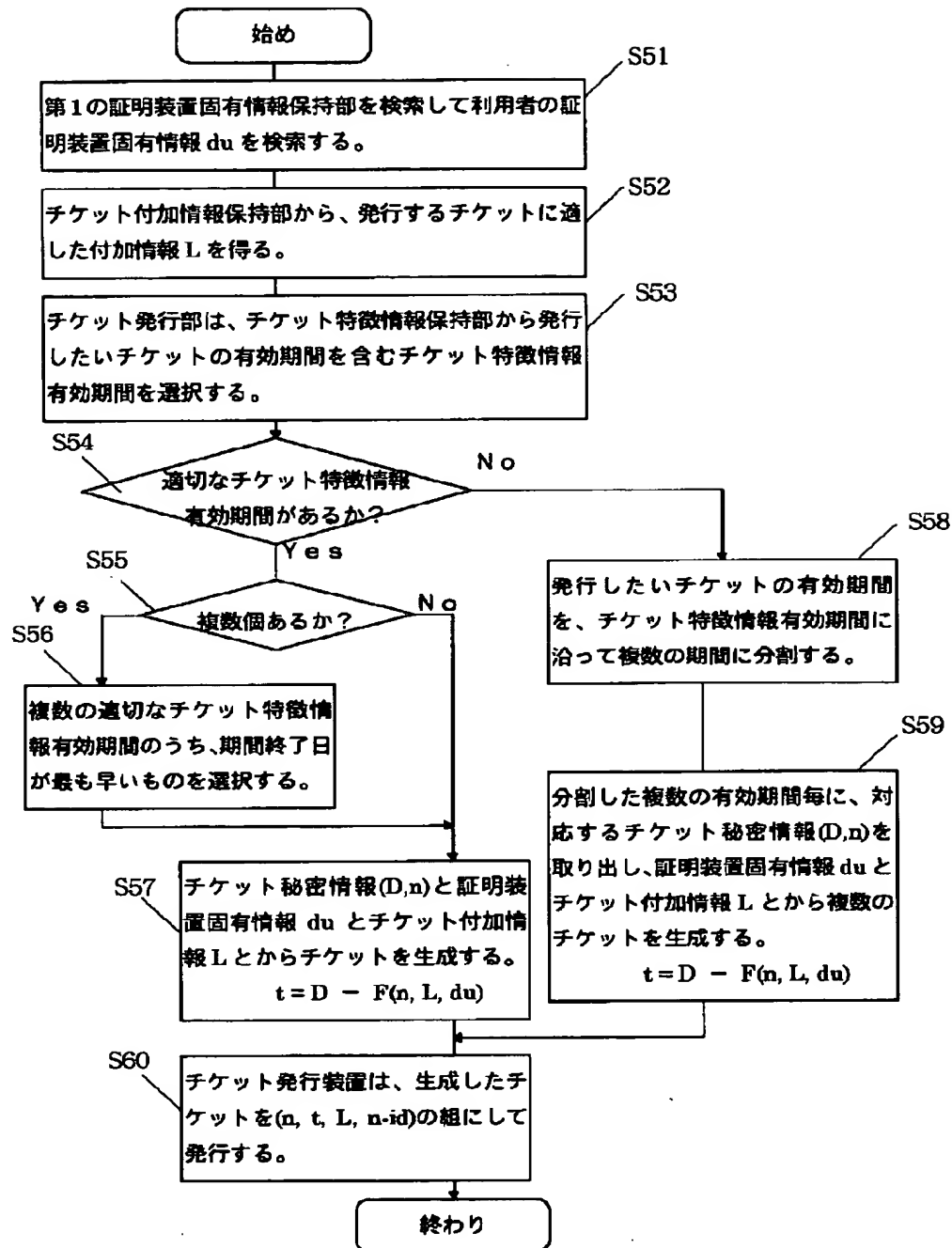
第2の実施例のチケット発行装置の処理の流れ

【図10】



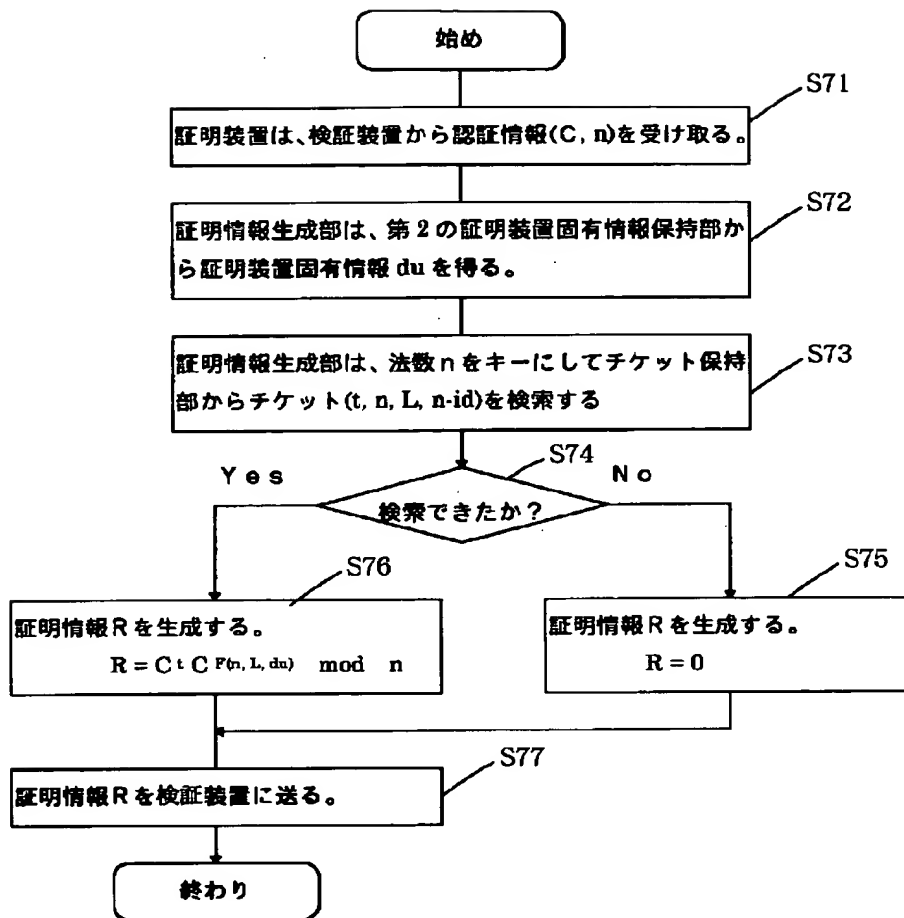
第3の実施例の構成図

【図13】



第3の実施例のチケット発行装置の処理の流れ

【図14】



第3の実施例の証明装置の処理の流れ

【図22】

チケット特徴情報有効期間 (term)	チケット秘密情報 (x)	チケット公開情報 (y)	法数 (p)
...
1997.7.1~1997.10.31	x7	y7	p7
1997.8.1~1997.11.30	x8	y8	p8
1997.9.1~1997.12.31	x9	y9	p9
1997.10.1~1998.1.31	x10	y10	p10
1997.11.1~1998.2.28	x11	y11	p11
1997.12.1~1998.3.31	x12	y12	p12
...
...

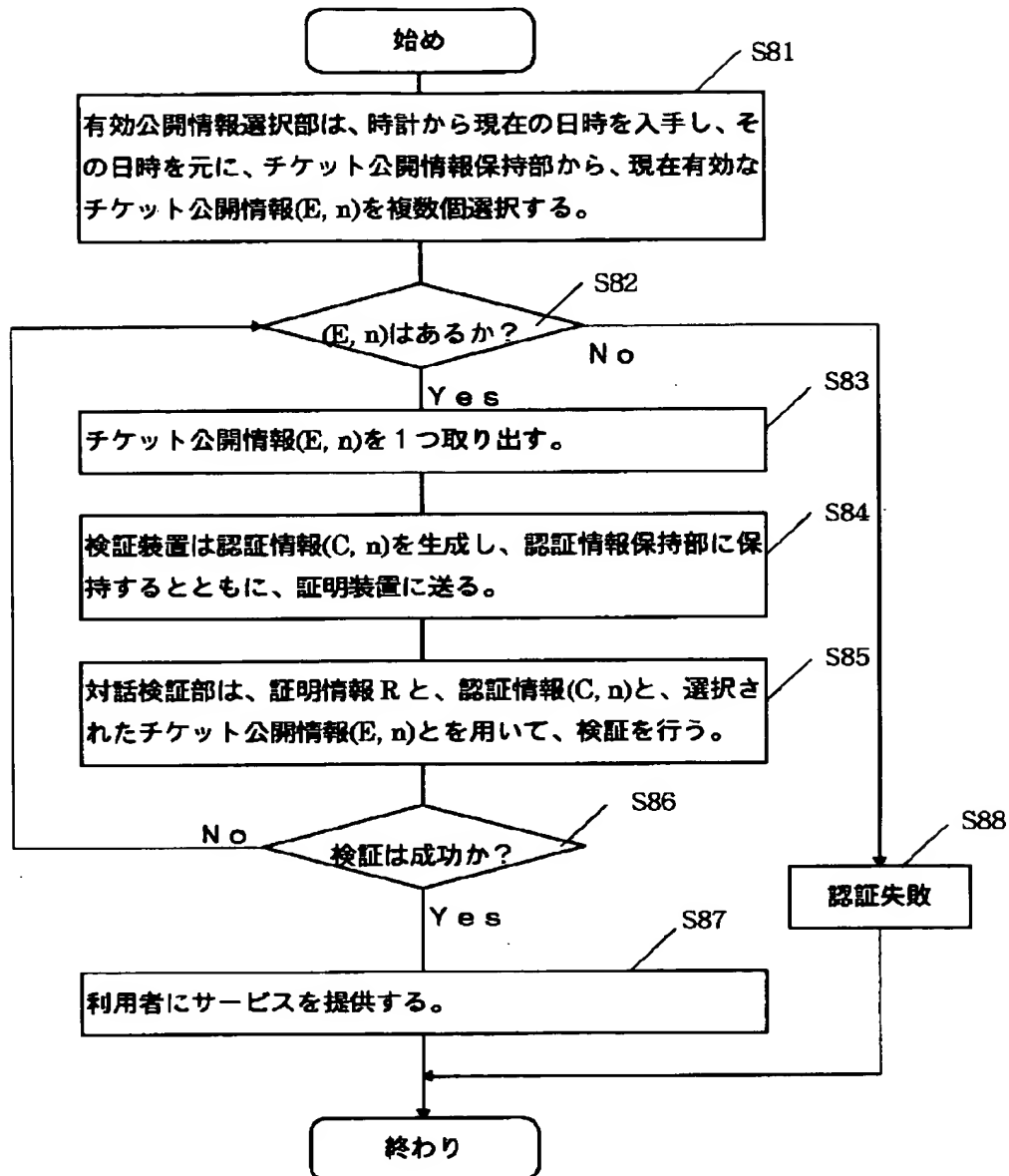
第5の実施例におけるチケット特徴情報保持部の例

【図23】

チケット特徴情報有効期間 (term)	チケット公開情報 (y)	法数 (p)
...
1997.7.1~1997.10.31	y7	p7
1997.8.1~1997.11.30	y8	p8
1997.9.1~1997.12.31	y9	p9
1997.10.1~1998.1.31	y10	p10
1997.11.1~1998.2.28	y11	p11
1997.12.1~1998.3.31	y12	p12
...
...

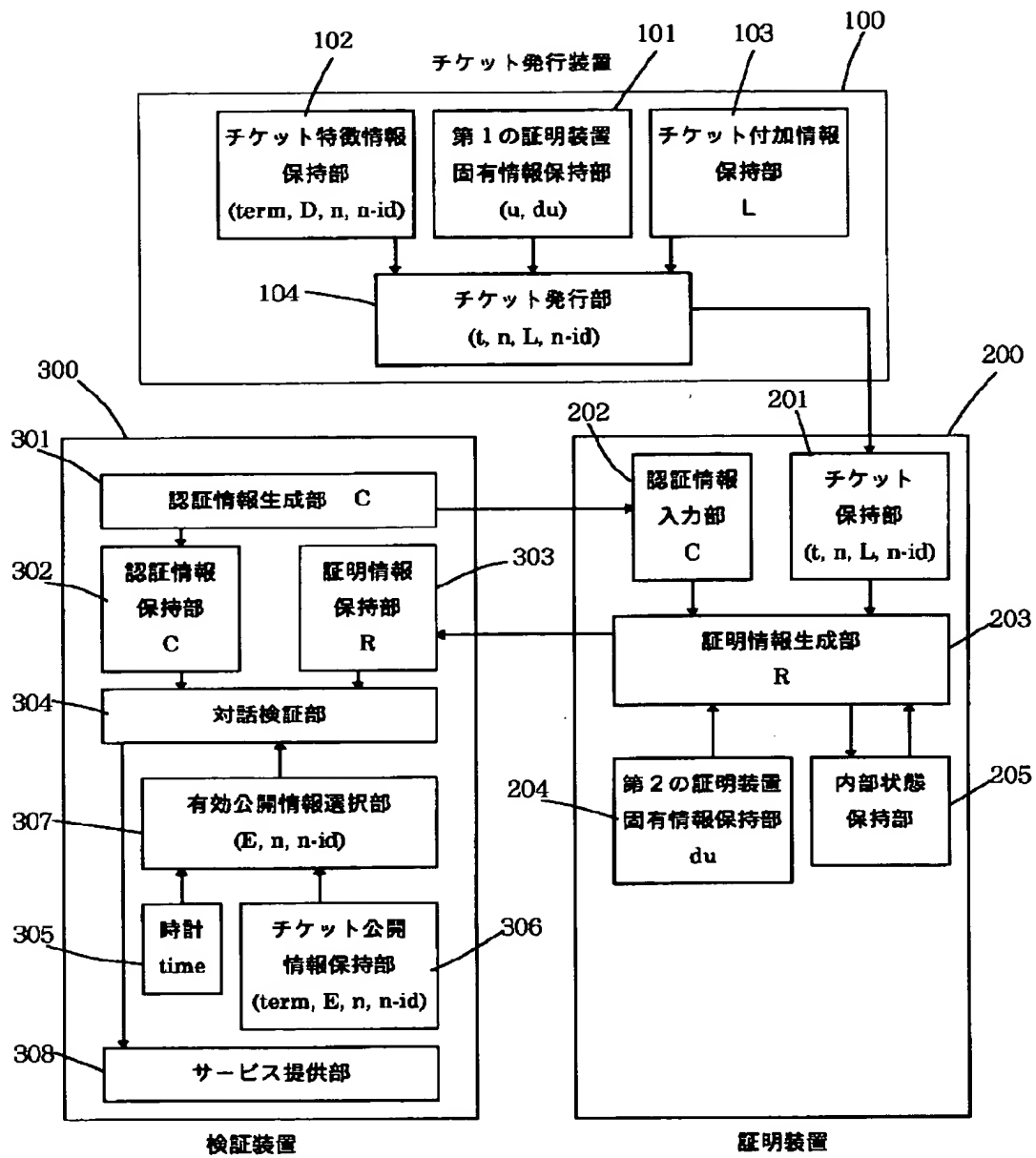
第6の実施例の検証装置のチケット公開情報保持部の例

【図 15】



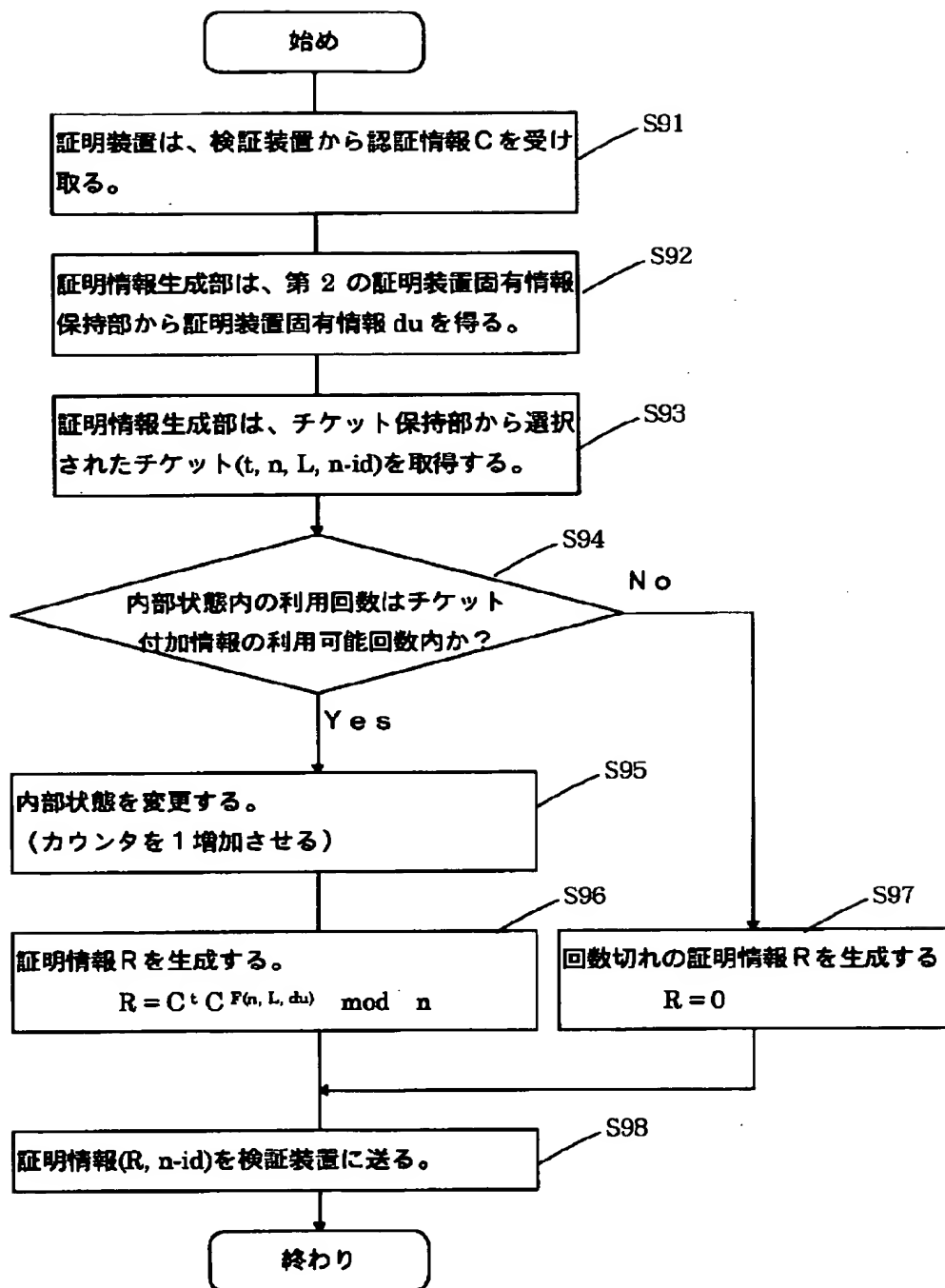
第 3 の実施例の検証装置の処理の流れ

【図16】



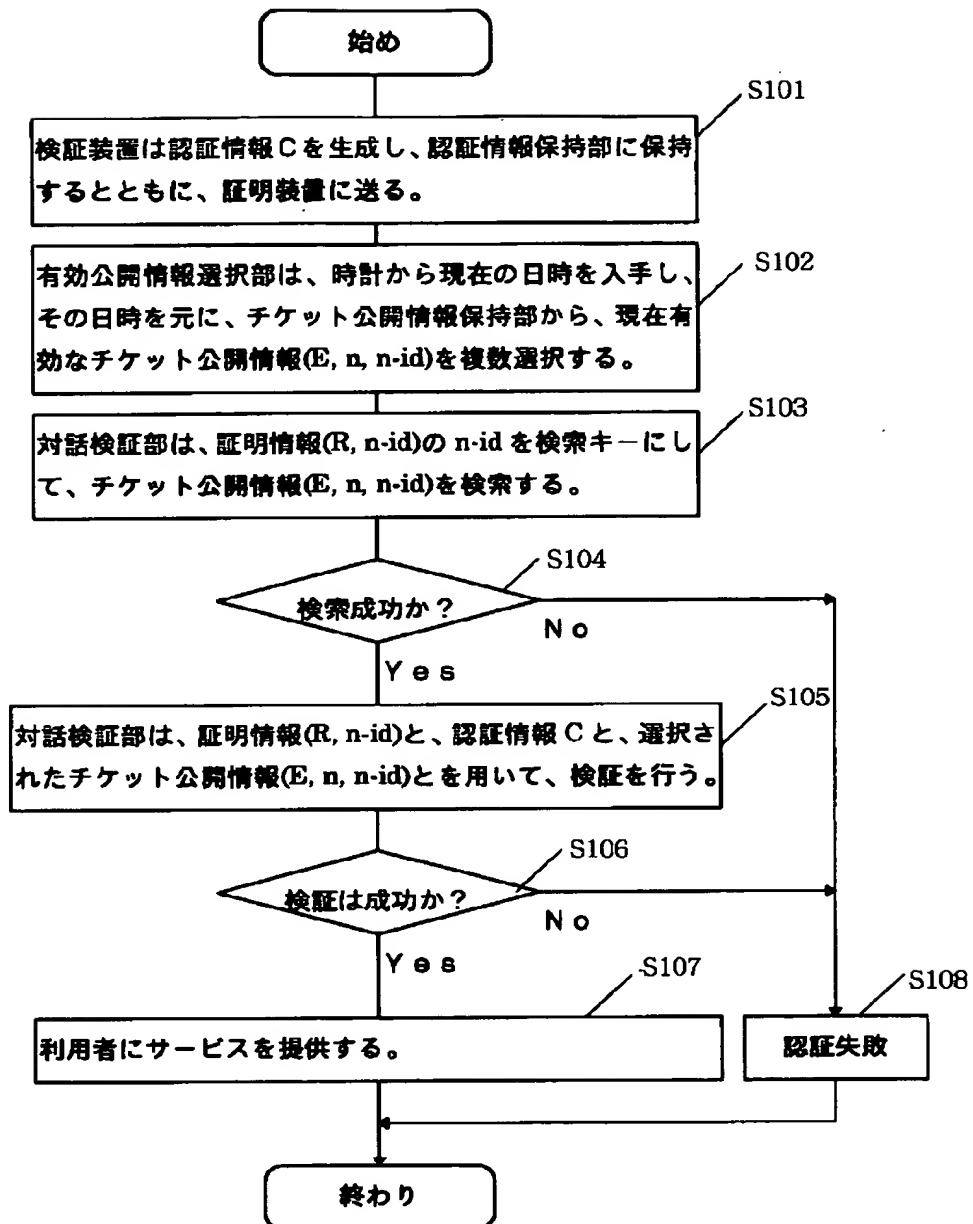
第4の実施例の構成図

【図 1 7】



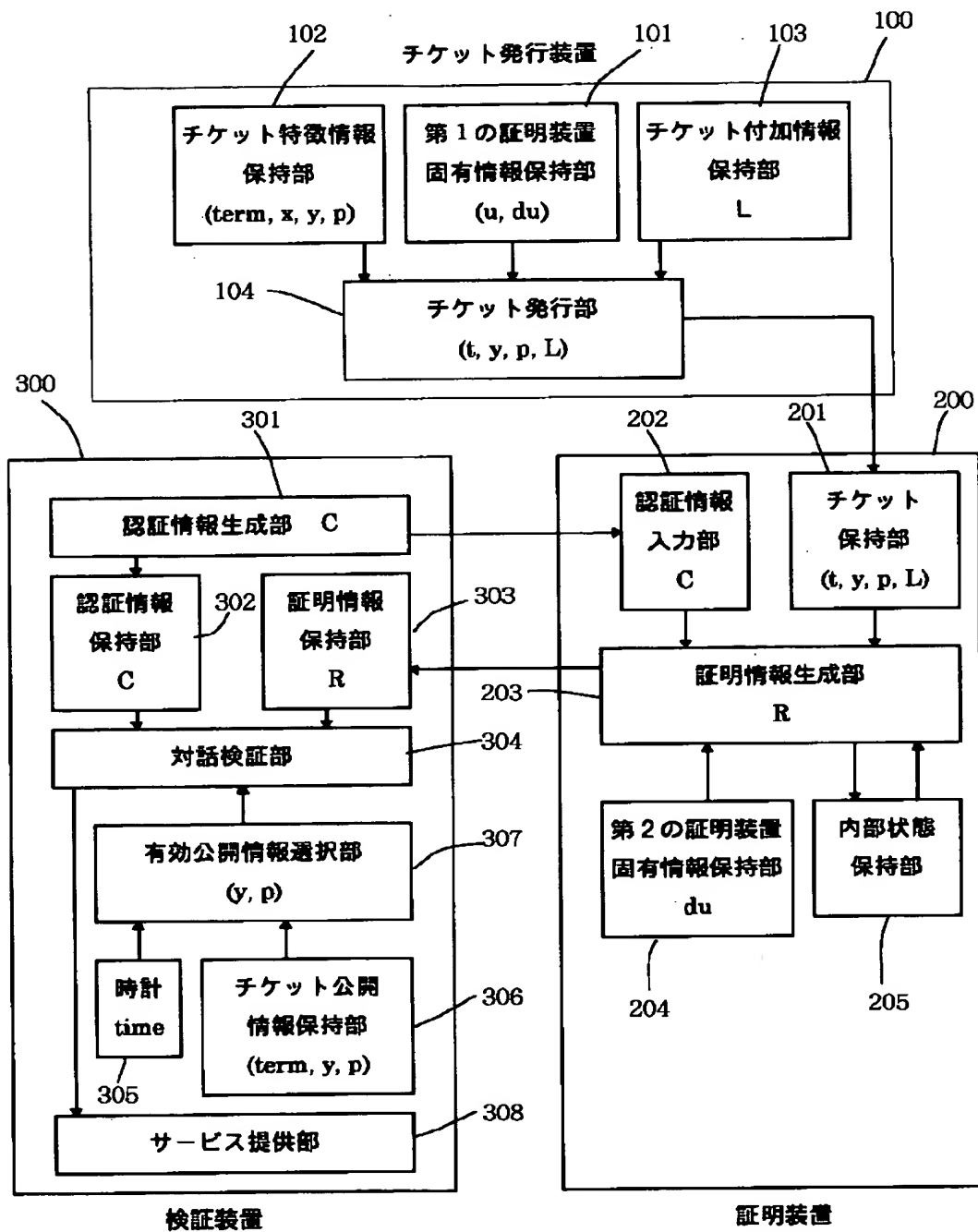
第4の実施例の証明装置の処理の流れ

【図 18】



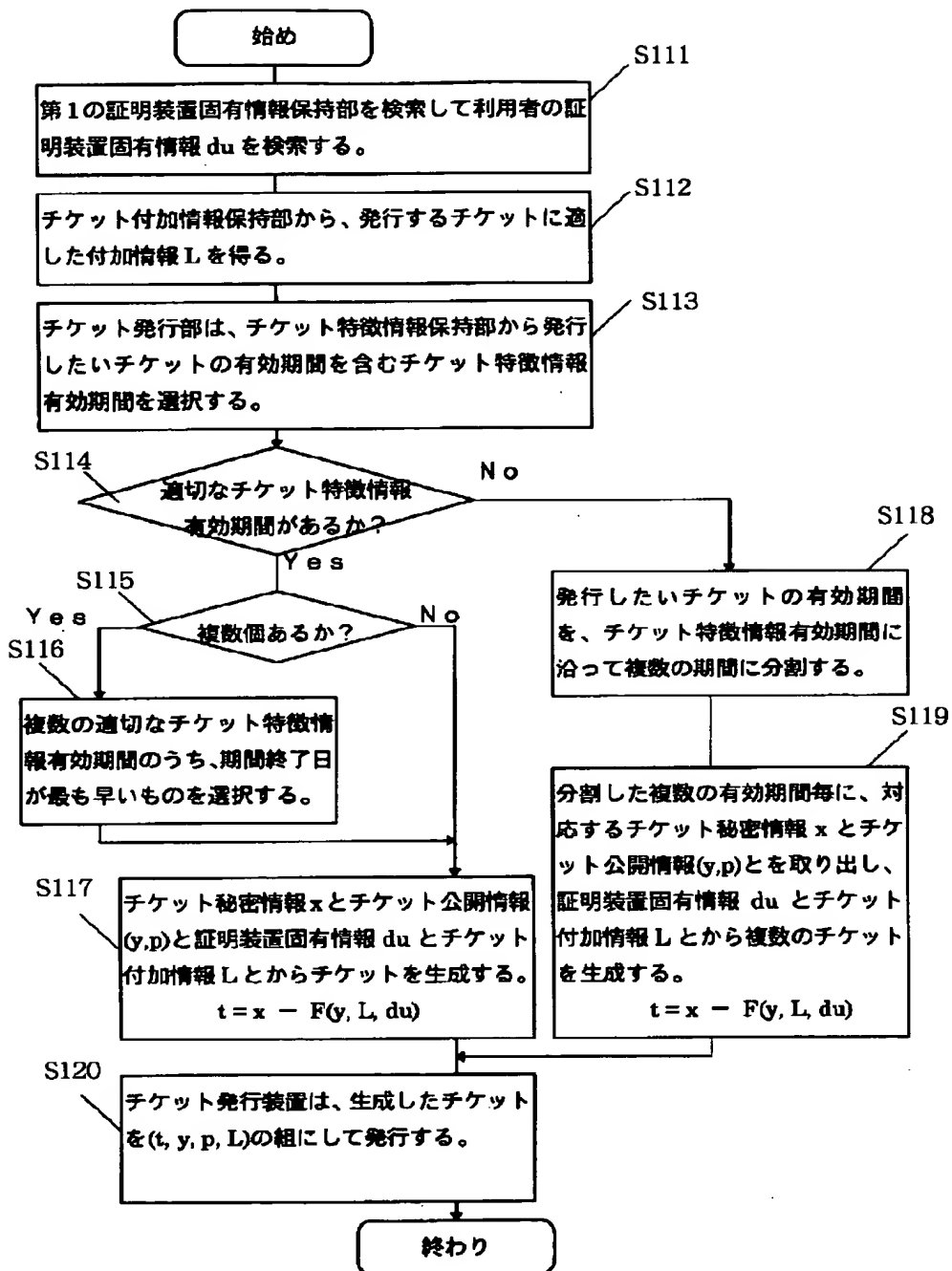
第4の実施例の検証装置の処理の流れ

【図 20】



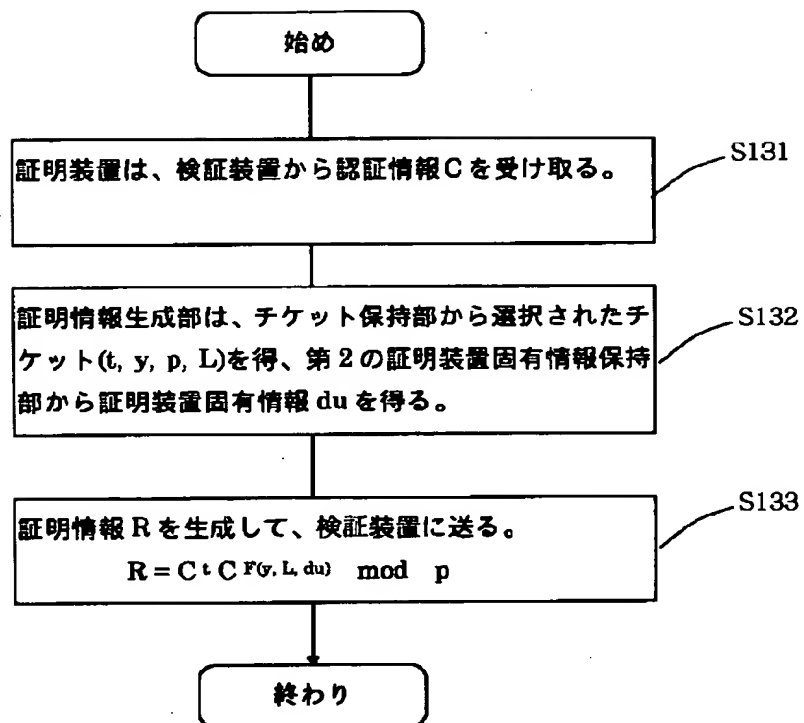
第 5 の実施例の構成図

【図 21】



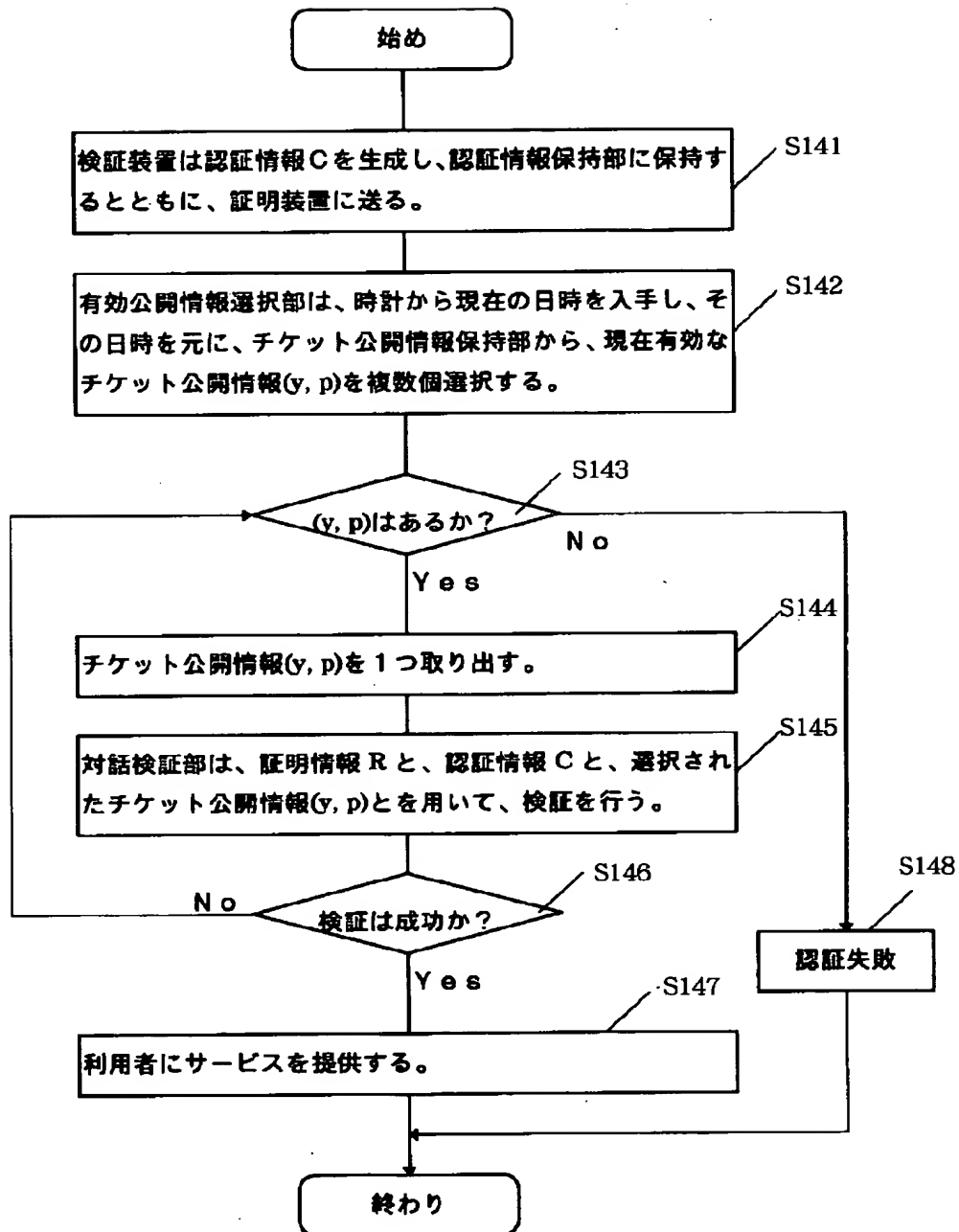
第5の実施例のチケット発行装置の処理の流れ

【図 24】



第5の実施例の証明装置の処理の流れ

【図 2 5】



第5の実施例の検証装置の処理の流れ

フロントページの続き

(51) Int. Cl. ⁶	識別記号	F I	
G 0 7 B 15/00		G 0 9 C 1/00	6 4 0 B
G 0 7 F 7/08			6 6 0 B
7/12		G 0 6 F 15/21	3 4 0 C
G 0 9 C 1/00	6 4 0	G 0 7 F 7/08	M
	6 6 0		C
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 B

(72) 発明者 谷口 慎一郎
 神奈川県足柄上郡中井町境430 グリーン
 テクなかい 富士ゼロックス株式会社内